AIR WAR COLLEGE

AIR UNIVERSITY

BYTES:
WEAPONS OF
MASS DISRUPTION

by

Michael W. Lamb, Sr.

Lt Col, USAF

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 APR 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Bytes: Weapons Of Mass Disruption	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**133**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Page

Introduction v
- Approach xii
- Key Questions xii

Chapter 1. Information Operations/Information Warfare—A Common Understanding 1
- Context 4
- The Information Weapon—Towards a Common Ground 7
- Information Warfare—The Spectrum of Conflict 14
- Cyberwar/Netwar: Weapon of Mass Destruction and/or Mass Disruption 16

Chapter 2. Some Parallels 21
- Deterrence 22
- Containment 25
- Flexible Response 26
- Counterforce/Countervalue 28
- Massive Retaliation/Mutually Assured Destruction 29
- A Comparison 30
- Information Warfare Weapons 32

Chapter 3. Offensive Information Warfare 35
- Policy 35
- Issues 38
- Strategy 39
- Constraints/Restraints 42
- The Commander and ROE 46
- A Different Look 51

Chapter 4. Deterrence—Strategy and Technology 53
- A Demonstrated Capability 57
- New Arsenals 58
- OODA loop or OODA point 62
- Vulnerabilities and Shared Threats 66

Chapter 5. Organization 78
- The Mission 78
- The Roles 80
- The Threats 82
- Civil Response 83
- Military Response 84
- Mutual Response 86
- Approach to Information War 88

Chapter 6. The National Plan—Towards a U.S. CONOPS? 92
- The National Plan 93
- Goals 94

The Programs 95
Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities. 95
Program 2: Detect Attacks and Unauthorized Intrusions. 96
Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law. 97
Program 4: Share Attack Warnings and Information in a Timely Manner. 98
Program 5: Create Capabilities for Response, Reconstitution, and Recovery. 98
Program 6: Enhance Research and Development in Support of Programs 1-5. 99
Program 7: Train and Employ Adequate Numbers of Information Security Specialists. 100
Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber-Security 101
Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8. 102
Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data 102
Conclusion 104
Some Final Recommendations 106
Annex A. Example IW Weapons 108
Computer Viruses 108
Worms 108
Trojan horses 108
Logic bombs 109
Trap doors 109
Chipping 109
Nano machines and Microbes 110
Electronic jamming 110
HERF Guns - EMP Bombs 110
Annex B. Common Definitions 112
Bibliography 116

Introduction

You bring me 10 hackers and within 90 days I'll bring this country [USA] to its knees.

- Mr. Jim Settle[1]

This is a Test

It was a typical late afternoon, just as many TV stations were broadcasting the news, many teenagers were logged on to the internet and chatting; a wife was reconciling her checking account online with her bank; a young man was engaged in an online game of Half Life Counterstrike; a retired couple were programming movies to watch on their DSP TV satellite receiver; and, at many university libraries students were searching worldwide databases for their class projects.

Suddenly, across computer screens and TVs there appeared a little figure dressed in white with a red cross on his chest, turning a disk. Every now and then the figure would stop, bend over, and give the appearance of examining a spot on the disk. After a second, the figure would straighten up and continue to search for another injured sector on the spinning disk. Then suddenly, entire screens went blank; there was no flickering or shrinking of the image that was characteristic of a power loss. Just as people were beginning to react, on the left side of the screen a figure begins to emerge. The peculiar figure attired from head to toe in green medieval armor and mounted on a bard horse, sports a long lance and carries a shield. The knight rides out into the center of the screen and once there, the horse turns until the small green knight, lance still held at a forty-five-degree angle, was facing head on. The figure pauses only long enough to lower his lance and tuck his shield up closer to his body. Then, with a quick swing of his feet, the green knight spurred his mount and charged forward. As the virtual knight loomed closer and grew larger, more and more details are revealed. Suddenly you realize the knight was not all green. Instead, the armor of the growing image blossoms into a motley pattern of light greens, dark greens, browns, tans, and splotches of black not at all unlike the camouflage pattern worn by today's combat soldiers. Even the bard protecting the knight's steed was adorned with the same pattern.

Only the shield clinched by the charging knight failed to conform to this scheme. The shield's background was as black as the rest of the screen. Upon that field, at a diagonal was the symbol of a silver lightning bolt, coursing its way from the upper right-hand corner almost down to the lower left. On one side of the bolt there is a yellow zero, on the other a one, numbers that represented the basic building blocks of all computer languages. Suddenly, as the knight fills more and more of the screen, many realize that this was not meant to be entertaining. Rather the symbol of military virtue, power, and untiring quests was a harbinger of disaster. Some attempt to look for the power switch, others change their TV channels to see the same knight advancing, and others remained captivated by what was unfolding—when suddenly, as if struck by a lightning bolt, not unlike the one adorning the knight's grim black shield, screens across the country go blank.[2]

Many look out their windows to see if there was indeed a power outage, many pick up their phones only to hear a busy signal tone, and others try to adjust their radios to local stations but only hear background noise. After forty-five minutes, a message appears across computer and TV screens alike—the dark knight announcing that what had happened was just a test. A test, reminiscent of days long ago when TV stations and radios conducted civil defense exercises. The message went on to state "Had this not been a test, your systems would not have been restored to you." Then suddenly computers again displayed familiar programs, on TVs were programs already in progress, radio station announcers were trying to determine what had happened and, now that phones were working again, were asking listeners to call in. This was a demonstration of an offensive information attack, a sample of a capability albeit small in its scope, intensity, and potential lethality. It was the first such demonstration to the world what the U.S. could do, not at all that much different than the explosion of the first hydrogen bomb.

The term "information warfare" has thus caught the attention of an entire generation of military thinkers. While the term encompasses both offensive and defensive measures, much of the imaginative thinking has concerned attacks on an adversary's command-and-control and information systems using methods as diverse as computer viruses, laser beams, and high-powered microwaves. Much of this thought goes into comprehending the possibilities, and maximizing the effects, of high technology in information warfare. For example, consider the consequences and effects if the following systems were disabled: financial markets, nuclear power plants, telephone systems, power distribution systems, traffic lights, or air traffic control and airline reservations systems.[3]

But one must understand the "why" one would use an information warfare attack. Information can be both the target and the weapon. As a matter of fact, information may be the most formidable weapon of the 21st century. Why then would an adversary use information as a weapon? Certainly the primary reason for an adversary to resort to information warfare is because the U.S. is increasingly more dependent on information in every aspect of its society. It is relatively cheap for an adversary to obtain for the "bang for the buck." Information warfare can have lethal and non-lethal effects depending upon target selection. It is the warfare of the future.

However, given the high degree of uncertainty in assessing the key enabling factors and constraints on using different strategies, the willingness to suffer the risks of failure, retaliation and escalation are also relevant to assessing which adversaries may prove most likely to develop and use such capabilities. For example, does the adversary have alternative means to pursue the objectives, which are less uncertain and risky? How painful are the perceived risks of failure,

retaliation and escalation? Analyzing who might choose to develop and use information warfare capabilities against the U.S. clearly presents a complex task.

For the U.S., information warfare enhances our power projection by reducing the adversary's will and capacity to make war. Further, its use as a precursor enhances conventional attacks and operations against a blinded and degraded adversary, thus decreasing an effective defense and counterattack. It provides the capability to turn inside an adversary's OODA loop, to act before the adversary can. Given that our adversaries will utilize information warfare to exploit U.S. vulnerabilities and impact our capability to dominate the battlespace, the U.S. needs information warfare to act as a counterbalance, a deterrent capability.

The ability to destroy with precision an adversary's command-and-control system, and the ability to attack his information infrastructure causes problems for the operational commander. The question of "what can it do" with information weaponry already has a myriad of answers. There are additional ones created daily. As technology advances, using bytes as weapons information war becomes more feasible and attractive. The important question is rapidly becoming "when shouldn't I use" these high-technology weapons?

Unfortunately, the responsibility to use lethal means rests with those who will execute such missions, the military. The military cannot allow its leaders to walk blindly down the information armory, choosing and employing these new information weapons without regard to their impact. They must consider the potential consequences of information warfare weapons. The targets selected may be compromised or disrupted or destroyed through non-lethal or lethal actions. The greater capacity these weapons have, the greater restraint they may demand. Military leadership cannot afford to wait until the adversary is at the very gates before assessing how to employ this information arsenal.

Most new weapons have been limited to some degree in their use by custom, legal restriction or self-imposed restraint. Chemical weapons were seen as so lethal and indiscriminate as to be banned by treaty. Nuclear weapons were so powerful that their use became almost unthinkable and the U.S. developed a separate policy and strategy for its use. The weapons of information warfare have effects, as potentially devastating as those of nuclear weapons, yet there has been relatively little closure in the debates on the implications of these newest technologies and their use in war. There are legal and practical limitations that the President or Secretary of Defense and, more specifically, the operational commander must consider before employing these technologies.

A final problem to consider, especially with this new, potentially highly destructive, technology is the problem of retaliation. The U.S. is the most information-dependent country in the world and, even if military systems are hardened, has the greatest vulnerability to information attacks. Recently, Time magazine said, "An infowar arms race could be one the U.S. would lose because it is already vulnerable to such attacks."[4] These attacks could take the form of escalation, or be acts of desperation. Just as Saddam Husayn launched Scud missiles in frustration during DESERT STORM, any adversary that found its information weapons ineffective against U.S. armed forces may direct them against civilian targets like the Internet, communication satellites, or undersea fiber optic cables. While these targets may not be militarily significant during war, they could prove politically sensitive or at least disruptive and have an impact on the national will. The U.S. needs to decide both its response and possible adversary responses to information attack. The impact of possible retaliation actions must also be considered in the selection or rejection of information weapons.

With its information infrastructures emerging as centers of gravity, the U.S. is faced with critical risk and opportunity. It needs to establish, and maintain, as a national objective the achievement of information dominance. Pursuit of that objective demands that some hard decisions be made soon, because the U.S. is probably the most dependent of nations upon information and its infrastructure. Currently the cost of access to information systems is extraordinarily low. On top of that, computer and communications technologies are advancing at a rapid pace, even more rapidly than the now famous Moore's Law.[5] These exponential advances compound the problems of protecting complex global infrastructures from attacks.

How should the U.S. integrate the many disparate information warfare efforts underway in DoD, elsewhere in the government, and those in the private sector? Some factors to consider for such integration are:

- A national objective of the significance and potential impact of information dominance requires top down establishment of a national strategy and governing policies. In effect, it must have focused leadership and an assigned responsibility for end-to-end consideration of all the essential and integrated components of a most complex national scheme.
- Although defensive and offensive actions will involve the private sector, a national security rather than private/commercial sector perspective must dominate strategy and policy formulation.
- The contributions of defensive and offensive actions to the objective of information dominance are mutually supporting and technically intermingled. Thus, the "protect and attack" dimensions of information warfare should be addressed as two integrated features of a single strategy. Together they constitute the challenge of ensuring information dominance.

These factors reflect the difficulties for leaders to develop a single, comprehensive, and integrated strategy that brings together the private, commercial, and government sectors. Logically, it follows from these factors that the U.S. has assigned many agencies some functional responsibility within the government for information warfare, most recently to U.S. Space Command. What is needed is a single responsible agency to coordinate activities such that the

U.S. will have timely planning, cohesive investment, and a reasonable chance of meeting national objectives.

In planning an overall information warfare strategy, it should be recognized that target information systems change rapidly and will change fundamentally in the near future. The U.S. needs to:

- Develop robust attack technologies capable of on-demand use against a range of target technologies/systems.
- Leverage intelligence community parallel technologies to access and process targets.
- Pursue long-term expert based study on improved techniques for computer attack, which increase on-demand effectiveness with reduced manpower investment.
- Pursue development and use of intelligent agents for attack mission.

Information warfare is an unprecedented capability that is not a continuation of industrial warfare. It is not just "command-and-control warfare"[6] nor is it just "cyberwar."[7] These are manifestations of information warfare, but as symptoms are neither the consequence nor the cause of a situation. These initial classifications are simple and temporary interpretations of something much more complex, fundamental and revolutionary. Information warfare is a developing reality that comes from a self-organizing process that has never been seen before. One problem with this new technology is that it is creating a new vocabulary with new terms with unknown inference.

These definitional problems raise institutional issues about who does what and how the Services need to organize to deal with information-related issues most effectively. The narrower definitions of information warfare essentially focus on attacking or protecting computers, databases, and the like lend themselves more readily to well-defined niches for organizations with manageable sets of tasks to perform. Unfortunately, defining information warfare narrowly does not justify all of the attention and hype that the subject is currently receiving. Neither does

it solve the larger problem of where that sort of "information warfare" fits in the overall scheme of things that are of interest to the Services and other Defense Agencies. This is particularly problematical in the emerging "gray areas" of national security that blur the distinctions between law enforcement and military responsibilities, war and peace, public versus private, and economic versus military security. To that end, this monograph will use a common terminology throughout. It will use the terms and definitions from Joint Publication 3-13, Joint Doctrine for Information Operations, dated 9 October 1998. These definitions are found in Annex B.

The early period of the nuclear age faced a similar situation. New terminology was developed such as “containment,” “countervalue targets,” “counterforce targets,” “deterrence,” “mutual assured destruction,” and “flexible response.” These new concepts were developed, along with the new policies and strategies that guided the use of these systems. Questions were raised about the limitations and controls that would be placed on the use of such weapons. How could one prevent this type of warfare? If it could not be prevented, when would one use these weapons offensively, and if so under what conditions? This is the analogous dilemma faced today when discussing information warfare.

While old words do not explain something new, it is possible examine history and draw some parallels that may aid discussion of information warfare. Such parallels can be derived by examination of the development of nuclear strategy and planning. Terms like deterrence, flexible response, assured destruction, counterforce and countervalue targeting might shed light on how strategic leaders view information warfare. Are there similarities? Could non-lethal means achieve as much or more than lethal means? Is information warfare a weapon of mass destruction (WMD)? Or is it a weapon of mass disruption?

Approach

This monograph will define offensive information warfare and associated technologies. It will then examine U.S. nuclear weapons policy, strategy, and doctrine to establish any similarities with offensive information warfare. It will also analyze the current U.S. policy, strategy, and doctrine to determine how these are integrated and what gaps (if any) exist. Lastly, it will assess how one might organize command-and-control elements in today's environment including new mission areas under homeland defense.

Key Questions

Information warfare encompasses offensive and defensive operations applicable to varying levels of war—strategic, operational, and tactical. This too was true for nuclear weapons. Taking a look at information warfare, one may ask:

- What new dimensions does offensive information warfare add to the existing arsenals? Can the history of nuclear weapons provide lessons learned?
- What technologies would one use (or avoid)?
- What strategy would one develop and apply? Are these similar to those one developed for using nuclear weapons and are there lessons learned that apply?
- Under what conditions would authorization be given to use offensive information warfare?
- What would be the Rules of Engagement (ROE) and what are the legal implications?

Each question can asked of any new weapon. As is true for any new weapon, warfighters must be provided clear guidelines for employment. Specifically, what are the constraints, and what are the limitations?

As with any offensive military action, one will need to assess what damage information warfare attacks have produced to verify the objectives that feeds back into the operational analysis. In information warfare one must assess battle damage in terms of effects and not just in terms of function and capability. Thus, planners must ask:

- How does one measure the effects of an information attack?
- How does technology help or hinder one's information warfare combat assessments?

Finally, while technology enables one to conduct offensive information warfare, when and how do policy, strategy, and doctrine come together? Will the U.S. ever conduct offensive information warfare or will it just 'carry a big stick' and will the use of information warfare transform into a deterrent not unlike the use of nuclear weapons?

Notes

[1] Mr. Settle is the former head of the FBI's computer security section, as reported in *The Australian*, 18 June 1996, pg. 59.
[2] Coyle, Harold W., *Cyberknights*, COMBAT, Tom Dougherty Associates, New York, NY, 2001.
[3] Sexton, Joanne, *A Combatant Commander's View of Information Warfare and Command-and-control Warfare*, Unpublished research paper, U.S. Naval War College, Newport, RI, 16 June 1995, pg. 3.
[4] Waller, Douglas, *Onward Cyber Soldiers*, Time, August 21, 1995, pp. 38-46.
[5] The observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore's Law, which Moore himself has blessed. Most experts, including Moore himself, expect Moore's Law to hold for at least another two decades.
[6] Command-and-Control Warfare — The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command-and-control capabilities, while protecting friendly command-and-control capabilities against such actions. Command-and-control warfare is an application of information warfare in military operations and is a subset of information warfare. Command-and-control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive:
a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.
b. C2-protect. Maintain effective command-and-control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command-and-control; electronic warfare; intelligence; military deception; operations security; psychological operations. (JP 3-13.1)
[7] Arquilla, John and Ronfeldt, David, *Cyberwar is Coming!*, The Journal Comparative Strategy, Taylor & Francis, Bristol, PA, 1993, Volume 12, no. 2, pp. 141-165. Cyberwar—any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. It includes the following modes of information warfare attack: infiltration, manipulation, direct assault, or raid. Infiltration is the penetration of the defenses of a software-controlled system such that the system can be manipulated, assaulted, or raided. Manipulation is the control of a system via its software that leaves the system intact, and then uses the capabilities of the system to do damage. For example, using an electric utility's software to turn off power. An assault is the destruction of software and data in the system, or attack on a system that damages the system capabilities. Includes viruses, overload of systems through e-mail (e-mail overflow), etc. Finally, a raid is the manipulation or acquisition of data within the system that leaves the system intact and results in transfer, destruction, or alteration of data. For example, stealing e-mail or taking password lists from a mail server. Also cyberwarfare.

Chapter 1

Information Operations/Information Warfare— A Common Understanding

Information warfare is about attacking the processes or process models in the infrastructure/infosphere. Attacks that pervert, corrupt, debase, or take advantage of the decision models affect the observe, orient, decide and act (OODA) loop.[8] In assessing information warfare, an understanding of the technology of control is particularly useful. Controls require a smaller, simplified model of the system to be managed or governed. Mechanical computers such as gear works, or advanced computers such as those in service today, provide process control. They also act as the modeling tool necessary to allow automation of various sorts. Application of these modeling tools has expanded from process control into decision-making. Such models include two dimensions (big, dynamic pieces of paper; software applications such as word processing or databasing) and three dimensions with time as a factor (complex space/time models; used for designing buildings, automobiles, nuclear weapons; or modeling the weather, global communication routing, financial markets, etc.). Technology for data and information processing is being used for calculations, simulations, and databases. Things that one used to do by hand are becoming increasingly less likely in most cases. Computer chips do many routine tasks while driving, adjusting temperatures in buildings, etc. As the reliance or dependence on technology increases, so does the trust factor one place in these technologies. They are routinely substituting human judgment and experience with automated decisions. Most humans forget that extrapolations or numeric models will not replace personal experience and engineering attention to detail based on testing. Despite mistakes, however, most people trust in the technology.

Information warfare takes advantage of and targets the frailties, shortcomings, and defects that have occurred as society evolved. It can be waged at any time, in any place, against any culture, and under any circumstance. Even the most primitive of societies has an infrastructure and dependency on certain routines and expectations. Attacks which deny a society, or subsection of a society, access, utilization, or benefit from an infrastructure in whole or part are referred to as "denial of service" (DOS) attacks. DOS attacks vary from the blowing up of bridges or communication-switching centers to mass attrition attacks on civilian populations in societies where the people are the infrastructure, such as an agrarian-oriented economies. In modern societies DOS attacks, also termed "information warfare," "netwar," or "cyberwar," can be hackers shutting down traffic control, attacking the software that controls communications switching, or mass flooding of the networks which manage social processes such as issuing tax returns or college registrations. Attack tools can vary from live "cracking" of systems to automated attacks with computer viruses or network-packet flooders. The intent of information warfare is to weaken or disable an opponent through denial, degradation, delay, or disruption in his routine processes. Conducting war in this fashion is intended to force failure in a process, or the control/automation of that process.

Rather than outright destruction/denial of an infrastructure/infosphere, distortion or corruption attacks can target processes (material, virtual, or human) and decision processes. This degrades the options or recommendations they provide or impair/damage models, where errors cascade and spread throughout the model. These psychological warfare sorts of attacks are far more difficult to accomplish because it requires a human touch to debase human decisions. Modern society has real-time demands for proximity, which increasingly forces automation of decisions, placing human judgment out of the loop entirely, trusting in the systems data and

operation in real-time. Dependencies are dynamic, and have thresholds. For example, alteration of a medical record to change a blood type doesn't impact the individual until that piece of information becomes critical to making an accurate decision. This means such attacks can occur on systems or information while unprotected because at the time of the attack, they seem unimportant.

Finally, there are numerous contributions that information technology makes to the process of political warfare: propaganda, disinformation, agitation, and social subversion. This variety of information warfare is a case of "politics by other means." One of the keys to making changes in a society or political economy is to create and provide an alternative, gaining supporters through persuasion or compulsion. Another is forcing the hand of the existing structure into making reactionary changes. The modern infosphere already provides numerous mechanisms for the creation, support, and growth of intentional communities, such as those created by design such as the “United States of America” or “cypherpunks.” Technology tools and communication channels provide unmatched tools for the creation and dissemination of propaganda and disinformation. They can organize groups, coordinate actions, and otherwise subvert the stability of social structures. No society is immune from information warfare actions. They can be waged from within or from without. The tools, methods, and cognitive models are usable cross-boundary. This allows a context shift to information war in varying modern, developing, or primitive societies, and from one sort upon another. The information warfare cognitive toolset even lends itself to a sort of an “a priori judo,” where a more primitive opponent can use the strength of their more advanced foe against itself.

Information warfare is not now a ready tool in the realist sense of a State versus State conflict. One should view these sorts of conflicts as being the exception rather than the rule.

States have a wide array of capabilities to decide their differences that are far less trouble to resort to than overt or covert warfare. Information warfare is a potentially high level-of-effort course of action in systems where the process of change is already built into the system's political processes. However, that does not preclude use of information warfare by non-State groups. They can effect change through information warfare on the political process in a way that other State actors cannot. A case could be made that the rise of the democratic concept is similar to the rise of the power of non-State actors. The democratic ideal pushed the authority boundary down just when the increased capability to use significant force also came within the means of the individual or sub-state organization. Power and authority have devolved from the State. It was only a matter of time until the prerogative of waging war, or engaging in significant technological conflict, could be exercised by non-state actors.

Context

Some analysts posit that information itself is the target in warfare, while others treat information as the weapon. Some see information as a critical resource. Others see it as a realm or an environment (infosphere), and others as a medium for military operations (infospace). Information can be considered the catalyst or control loop in a process, but one must realize that information can be used over and over again. Information warfare is a new and unprecedented situation. Information warfare is not a continuation of traditional warfare. The problem is that one talks about information warfare using terms that have well known connotations. But it is difficult to talk about something completely new using words that bring with them specific understandings. For example, the early period of the automobile was called a “horseless carriage” as the only way to define its essential quality. As the horse was the primary mode of transportation, people described the car as a carriage without a horse. One faces the same

dilemma when discussing information warfare. Old words, ways, or processes do not always explain something new. The danger is that the use of familiar words misrepresents and masks the true extent of the revolution that will have to take place. If one is to retain a military capacity in the new physical, social and cognitive space of information warfare, then one must understand its unique attributes.

Information warfare has become the new post-Cold War era national security catch phrase. Despite its rise in prominence among the concerns of national leaders and increased public discussion, information warfare remains an ambiguous and vague concept that has been used in a variety of contexts. Much of the discussion surrounding information warfare has focused primarily on the means of information warfare (organization and resources). Meanwhile the scope and meaning of information warfare has remained largely undefined. Therefore, a clear definition of information warfare is essential.

Information warfare in its broadest sense is a struggle that involves the communications process. It is a struggle that began with the dawn of human communication and conflict. Over the past few decades, however, the rapid rise in information and communication technologies and their increasing primacy has revolutionized the communications process. This has multiplied the significance and implications of information warfare. A modern society's communication and information processes are now composed of four critical interrelated infrastructures:

(1) The power grid.
(2) The communications infrastructure.
(3) The financial infrastructure.
(4) The transportation infrastructure.

Electricity, and thus the power grid, is the foundations of the entire system. Without electricity nothing works and one is back to using semaphore or smoke signals. The

communications infrastructure requires power and provides the ability to exchange information for news, business transactions, research, etc. The financial infrastructure requires power and communications and allows for the electronic flow of money. The transportation infrastructure, including the air traffic control system and the train routing systems, also requires the power and communications infrastructures. This allows for rapid and massive transportation of people, goods, and services throughout the nation. A modern battle over the communications process involves all of these infrastructures. Information warfare includes the electricity that powers homes and hospitals, the phones, faxes, and computers are used to communicate and share information, move trillions of dollars that drives the economy, and move trains and planes from one place to another. The new attention given to information warfare does not mark the start of a new form of conflict, as some have implied; rather, it marks a significant change in the implications of an old one.

The Brown Commission defines information warfare as "activities undertaken by government, groups, or individuals to gain electronic access to information systems in other countries ... as well as activities undertaken to protect against it."[9] This definition is too simple, overly broad, and runs the risk of confusing mischief and crime with warfare. Without distinguishing between crime, mischief and war, the DoD might find itself launching a counter-offensive against a teenager. The definition does not account for a physical assault (i.e. old-fashioned bombing) of the nation's information infrastructure.

> Information warfare is aimed at affecting the adversary's cognitive and technical abilities to use information while protecting our own—to control and exploit the information environment. In some ways it is technologically independent in that operations can be conducted via any of the media of war, not just cyberspace, to attain that key objective of weakening the adversary will, but in other ways the new medium of cyberspace offers a particularly rich environment through which one can reach those elusive targets, the adversary's will and capability, via the

> various entry ways and connecting points in the information environment, whether they be hardware, software, or wetware.[10]

Information warfare must be considered what it is called, warfare. It is the application of destructive force on a large scale against information assets and systems. It is aimed at the computers and networks that support the four critical infrastructures. However, the definition given by the Brown Commission highlights one important fact that one must protect against computer intrusion. Even on a smaller scale, this has become one of national security interest and is important in the current debates about information warfare.

The Information Weapon—Towards a Common Ground

All humans engaged in war, unassisted or enhanced by information systems, constitute what one can label as a living information war model. Information flows through, and is processed, by one's mental systems. In an information war model the flow is holistic, interactive, and an intertwined systems of systems. It can exist at all levels, the micro-level (unassisted individual) to macro-level (technologically enhanced organizations), which multiplies the potential for interactive complexity in larger and more collective systems.

Clausewitz reminds us that war is an act of force to compel the will of an adversary and states that "intellect is a clear, continuous vital contribution,"[11] inferring the connection between intellect and will. Sun Tzu speaks of subduing the adversary's will as the "acme of skill."[12] In fact, Clausewitz recognizes the fundamental human nature of war as "nothing but a duel on a larger scale."[13] As the will, emotion, and spirit reside together (a triad), Clausewitz recognized their relationship to information stating "the step is always long from cognition to volition, from knowledge to ability. The most powerful springs of action in men lie in his emotions."[14] Sun Tzu also wrote at great length about the informational impact on the will of an adversary. He is

customarily interpreted as emphasizing intelligence and deception. In a larger sense Sun Tzu is describing the mental and intellectual clash that is manifest in the clash of wills.

Physical warfare concentrates on compelling the adversary's will by diminishing his physical war making ability. Information warfare bears on the adversary's will through his mental and intellectual subsystems. But it can, if applied properly, have tremendously disruptive or destructive effects. It can corrupt or shatter his information-based infrastructure and the strategic cohesion that sustains him. The inherent non-lethal nature of pure information warfare makes new options available for the disruption of the adversary's entire interactive societal system by disabling key information based subsystems. In that vein, broad physical factors and broad mental and informational factors are synergized to leverage greater power. Thus, information warfare may be applied in three control roles to leverage power by:

- Enabling or enhancing one's physical force, or by diminishing the adversary's physical force.
- Directly attacking the adversary's will.
- Directly attacking adversary information not related to physical force, but with definite bearing on the adversary's overall ability and/or will.

Information warfare consists of "actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems while defending one's own."[15] This definition brings to light an often overlooked and crucial fact when discussing information warfare. It consists of both offensive and defensive components. Launching a information warfare assault doesn't necessarily mean using nefarious techniques to "hack," or penetrate without permission, a computer system. In fact, many of the digital tools in a infowarrior's arsenal are simply everyday devices, expressed in the bytes of 0's and 1's of computer language, that make a computer network like the Internet such a wonder of communications.

Not unlike the hypothetical assault described at the beginning of this monograph, for example, the Stock Exchange's computers could have been put out of action by an "electronic-mail bomb." First the attacker would break into the system of a company that manages the links between the Exchange and the Internet. The attacker would toy with the service provider's computers so that they routed millions of E-mail messages, generated from the attacker's computer to the Exchange. If the flood of false E-mail is large enough, the Exchange's Internet connection, and possibly its own computers, would become overloaded and eventually shut down.

In another example, shutting off a city's power might be a simple matter of guessing, with help from a personal computer, the password needed to enter the local electric company's computer system. Then it's a matter of commanding it to flip the city's "off" switch. Password "dictionaries," which generate hundreds of possible words or combinations of letters, are easily obtainable as freeware. An attacker could simply dial in the power company's system and run the dictionary program until it chanced upon the right code causing mass disruption throughout.

Infowarriors might also break into the air traffic control system by "hijacking" a password. How? Simply by waiting for someone who's manning a computer station to, say, get up for a five minute break without exiting the program he's working on and turning off his machine. This is a favorite among college students that operate huge, multi-user systems. Once inside a system, a skilled hacker can control it. Or how about the cleaning out of bank accounts? A "logic bomb," which is a program hidden within a computer and set to activate at some point in the future, destroying designated files might do the trick. So might a "data-service" attack that involves convincing a computer network to share its information with an intruder's computer.

If some form of computer security doesn't protect the network, there is no way to prevent a machine outside the network from requesting and receiving data. Some information warfare experts would include other forms of digitized assault under the nomen "information warfare." In addition to attacking the inner workings of computers, information warfare could also mean the use of information technology on the battlefield or the use of microwaves to block wireless data transmissions.

The National Security Agency (NSA), the federal agency that concentrates on the use of information technology, focuses more on the danger that militants with computers pose to the U.S. national security apparatus. In a 1996 General Accounting Office (GAO) report, the agency estimates that more than 120 countries now have "computer attack capabilities" for attempting to seize control of Pentagon computers in a way that could "seriously degrade the nation's ability to deploy and sustain military forces.".[16] According to the direst of information warfare theories, all computer systems are vulnerable to attack. The challenge facing leaders in charge of potential targets is deciding whether a glitch in a computer system means that somebody somewhere innocently pushed the wrong button or that the first shot has been fired in an information warfare attack. Moreover, since trap doors, Trojan horses, logic bombs and other devices can be placed in systems in advance of their triggering, the first shot may have been fired months or even years in advance of the harm it may cause. At that point, there is less than zero warning time for one to learn of the attack, except after it has been accomplished.

The primacy of information technology in recent years has had an unfortunate side effect. It has generated a whole new set of hazy jargon in an area that already has a tradition of giddy jargon and acronyms. Part of this can be dismissed as relatively innocent word play typified by expressions such as "cyberspace," "cyberwar," "information highway," "infosphere," and almost

any imaginable noun preceded by the adjective "virtual."[17] Arguably, there could even be some value in reminding military commanders that their concerns must extend beyond the physical boundaries of the immediate conflict (e.g., cyberspace) and include possibilities other than physical attacks (e.g., cyberwar).

Intellectually, the point is easy to understand, but it raises some troublesome organizational issues. In particular, computer "hacking" attacks can be launched from virtually any place against any other place on the earth, or perhaps above it, thereby allowing any information-intensive conflict to become as "global" as the adversaries choose to make it. Beyond the merely annoying or the marginally useful, however, lies a more serious concern. The danger is that the way the problem is discussed can interfere with the way the substantive issues are framed and analyzed. That could easily lead to poor decisions that have unanticipated consequences. For example, the futurist view of the overwhelming importance of information in future war is appealing but needs to be subjected to rigorous critical analysis before being accepted as fact.

An important example is the expression "information warfare" itself, which is vague to the point of being misleading because various organizations are defining it differently and emphasizing different facets of the problem.[18] Others tend to emphasize electronic attack and defense and exclude the broader notion of "information operations" from the definition of information warfare. Still others forgo the expression of information warfare entirely and use more precise language. Probing for an acceptable definition appears to have absorbed an inordinate amount of the defense community's attention in recent years, yet ambiguities still remain.[19] The basic point of contention seems to be the scope of "information warfare." One side limits itself to conducting or defending against "electronic attacks" on computers and related

information systems. The other side includes the whole spectrum of possibilities for using information effectively in warfare and denying adversaries the same capability.

As noted, broad interpretations of “information war" cut across the entire spectrum of military operations and involve quite disparate kinds of things such as: military and civilian computer security, support for targeting precision-guided weapons, defense suppression, and command-and-control attacks that interfere with all manner of adversary computer systems. If one were to ask who is responsible for this kind of "information warfare," the answer has to be "everybody." Ironically, that is almost certainly the right answer to the wrong question. The right question is how does "information warfare" affect the conduct of military operations and, more broadly, long-term U.S. security?

The jargon of the debate is also routinely exploited in turf and budget battles. This is one of the most familiar ways in which jargon is used and abused in organizations. The new jargon represents an indicator that something new is afoot and that, to be among the experts, one has to be able to "talk the talk." This tends to be the precursor to laying claim to the turf and the associated budgets. In times of shrinking defense budgets, when roles and missions of all the Services and defense-related agencies are up for grabs, these kinds of turf battles seriously affect not just the relative importance of organizations but their very survival. Adopting trendy language is a serious weapon in these wars. Potential organizational competitors may not be reassured by appeasing language in position papers and PowerPoint briefings in which one group disavows any intent to dominate a hot new area. Thus, what appear to be harmless word games mask the most serious kind of hardball. Unfortunately, such misuse of language does little if anything to help solve the serious problems of deciding what should be done and by whom to deal with the very real problems of protecting U.S. security in an information-rich world.

Even more fundamentally, focusing on "information warfare" leads to a confusion of means and ends that tends to stand basic strategic thinking, the definition of overall objectives followed by the evaluation of various alternative means to accomplish those objectives, on its head. This is another area in which reassuring words on PowerPoint slides are not likely to be sufficient to overcome the institutional pressures. That leads to a focus on inappropriate and intermediate measures of effectiveness for the "information war" at the risk of losing sight of the linkage to more fundamental objectives. To recognize this danger, one should remember how "body counts" were presented as military measures of effectiveness in the Vietnam War. Hopefully, "byte counts" or something equally crude will never become the body counts of the new century. But war games revolving around information continue to provide anecdotal examples of analysts and planners using inappropriate measure of effectiveness to prove they were winning the "information war." These have little reference to the ends that information is intended to serve in combat.

An example of this particular phenomenon at work is the expression "information dominance," which is frequently cited as a top priority goal of information warfare. Now, the notion that one should know as much as possible about one's adversaries, as well as one's own forces, while trying to keep the adversary as much in the dark as possible is hardly a surprise to any student of military affairs. Sun Tzu emphasized the relative importance of what amounts to "information dominance" nearly 2,500 years ago without burdening readers with the jargon. If that is all information dominance means, then it amounts to a needless repetition that adds nothing of substance to present-day discussions of military strategy and operations.

Information Warfare—The Spectrum of Conflict

The Gulf War illustrated the importance of information dominance from infrastructures to national defense. The domination of Iraq's information and communications ensured victory over a well-armed military force with minimum allied losses. Most students of warfare have drawn similar conclusions. Offensive information warfare uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. Many understand that there is little in the way of special equipment required to launch information warfare attacks on U.S. computer systems. The basic attack tools, computer, modem, telephone, and software, are essentially the same as those used by hackers and criminals. When compared to the military forces and weapons that in the past threatened U.S. infrastructures, information warfare tools are cheap and readily available to anyone who could afford them.

If the basic information warfare tools and skills are common across the spectrum, what may distinguish recreational hackers from infowarriors is organization. In other words, an information warfare attack against U.S. infrastructures may be little more than a series of hacker attacks conducted against carefully chosen and thoroughly scrutinized targets, synchronized in time, to accomplish specific objectives. For an adversary willing to take more risks, these attacks could be combined with physical attacks, against facilities or against human targets. Such an effort could paralyze or panic large segments of society, damage one's capability to respond to incidents such as disabling the 911 system or emergency communications, hamper one's ability to deploy conventional military forces, or otherwise limit the freedom of action of one's national leadership.

Terrorists frequently choose prominent targets that produce little physical impact beyond the target itself, but widespread psychological impact. For a physical attack on infrastructures, less spectacular targets could be chosen, such as switching stations, communications antennas,

pipelines, transformers, pumping stations, and underground cables. Many facilities whose physical damage or destruction would have a disruptive effect on an infrastructure are purposely located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time to discover the nature of the damage. In the absence of casualties, it might be some time before the attacks are reported. Even when they are reported, each incident is at first a local event, and if several such events occur over a period of weeks or months it may take some time before such events are recognized as part of a pattern. Recognition that an attack is in progress could be delayed even if physical attacks were to occur simultaneously. If the targets were spread across several jurisdictions and no mass casualties were produced, then it may not generate "breaking news" at the national level.

The chances of immediately discovering that a concerted information warfare attack is in progress are today even slimmer. Computer intrusions do not announce their presence the way a bomb does. Depending on the skill of the intruder and the technology and training available to their own system administrators, individual companies whose networks are penetrated may or may not detect an intrusion. Intrusions that are discovered may or may not be reported to law enforcement authorities. These authorities may or may not have the resources to investigate them and conclude whether they are the work of an insider, a hacker, a criminal, or someone truly bent on harming the infrastructure. It sometimes takes months, even years, to determine the significance of individual computer attacks. In the highly publicized 1994 Rome Labs case, the main intruder, a London teenager, was caught in the act; but his alleged accomplice and mentor, who turned out to be a Welsh computer specialist only a couple of years older, was not identified and arrested until some two years later.[20]

It is difficult to analyze incidents in the absence of intrusion detection tools and uniform reporting of incidents. It is conceivable that an orchestrated attack against U.S. infrastructures could be under way for some time before it is recognized as such and the attacker's motives and objectives can be construed. Information warfare attacks thus can run across the gamut and spectrum of conflict. Attacks can also vary in intensity and scope, making them difficult to detect and later pinpoint its source. As shown here in Figure 1, information warfare runs across the spectrum of conflict and activities from peace operations through strategic nuclear war. The intensity of activity reaches a peak when a situation evolves from a crisis into a conflict. What this points out to the warfighter and campaign planner is that information warfare is present across the spectrum of conflict and should be accounted for defensively and offensively. Such planning is as equally important as communications, logistics, and force planning.

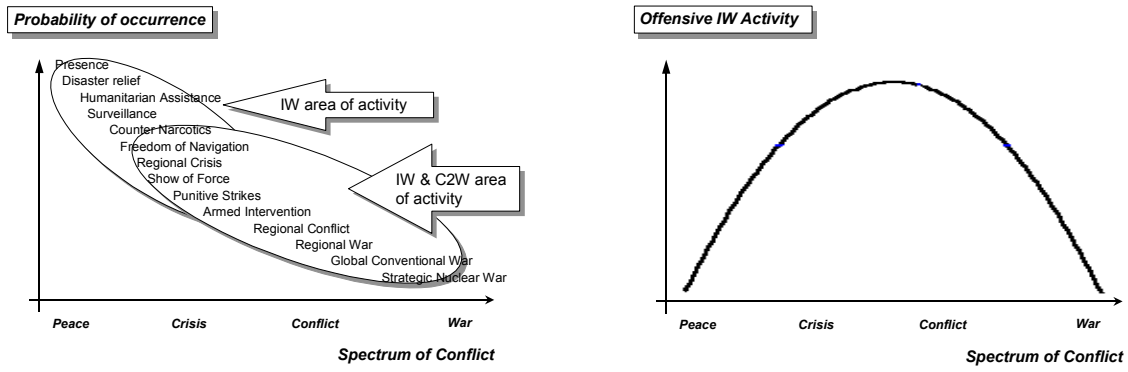

Figure 1. Information Warfare and the Spectrum of Conflict[21]

Cyberwar/Netwar: Weapon of Mass Destruction and/or Mass Disruption

Since information is the only resource that can exist simultaneously in more than one place, and can be moved at the speed of light, it transcends the time and space limits on physical force. This transforms the principles of concentration and economy of force. Operations tempo

will be significantly altered, not just in the physical realm, but also in a synergistic application of all the roles of information war. Whole new viewpoints emerge for the definitions of depth and reach. It is probable from the purist view of information warfare that the boundaries of rear, close, and deep areas disappear. Information warfare will likely offer effects that transcend the functional levels of war. New strategic and operational options for deterrence, preemption, conflict, termination, and peace maintenance are created.

Cyberwar is a component of "conventional" military contests; that part of the conflict oriented toward collection, analysis, communication, and use of knowledge. Information technology is a component of cyberwar that makes distribution of information possible, but the second order effect of networking is at least as significant. Hierarchal structures of military systems will become much less exclusive, as networks will often replace hierarchies in conflict. The impact on such hierarchal structures will allow commanders to go directly from the operational level to the tactical level, or directly to the warfighter on the battlefield. Use of this capability will be a huge temptation, especially in time critical circumstances where the commander can override the existing system hierarchy and chain of command. In addition, not all data may be available to a commander because of a constrained flow of data, that is its bandwidth. In fact, all the bandwidth available in Operation ALLIED FORCE was consumed by only 10% of those deployed.[22] Data could be filtered, or more problematic would be a commander making a decision on limited sources of data instead of a common operational picture of the battlespace. Such interventions like these will need to be addressed and carefully defined in the Rules of Engagement.

Cyberwar refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It

means trying to know everything about an adversary while keeping the adversary from knowing much about you. It means turning the balance of information and knowledge to one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.

This form of warfare may involve diverse technologies, notably for command-and-control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend-or-foe, and for "smart" weapons systems. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits. As an innovation in warfare, cyberwar may be to the 21st century what blitzkrieg was to the 20th century. It is an integration of existing technological advances. At a minimum, cyberwar represents an extension of the traditional importance of obtaining information in war: having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the adversary before he does the same to you.

Netwar has much less to do with exploitation or destruction of information systems. Cyberwar is that part of the military operation with conventional forces and battles while netwar is information warfare without military forces or physical battles. Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, delay, deny, degrade, or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.

Netwar represents a new entry on the spectrum of conflict that spans economic, political, and social, as well as military forms of "war." In contrast to economic wars that target the production and distribution of goods, and political wars that aim at the leadership and institutions of a government, netwars would be distinguished by their targeting of information and communications. Netwars can take various forms. Some may occur between the governments of rival nation-states. Other forms of netwar may arise between governments and non-state actors. For example, netwar may be waged by governments against illegal groups involved in terrorism, proliferation of weapons of mass destruction or drug smuggling. Advocacy groups involving, for example, environmental, human rights or religious issues, may wage it against the policies of specific governments. Non-state actors may or may not be associated with nations, and in some cases they may be organized into vast transnational coalitions. Some netwars will involve military issues, such as nuclear proliferation, drug smuggling and antiterrorism, because of the potential threats they pose to international order and national security. Netwars are not real wars, as traditionally defined, but netwar might be developed into an instrument for trying to prevent a real war from arising. Deterrence in a chaotic world may become as much a function of one's information warfare posture and presence as of one's force posture and presence.

The discussion of information warfare includes a myriad of new terms and jargon. The next chapter will examine nuclear strategy terminology of and examine any similarities. This examination may shed light on the roles and missions that information warfare plays in the Post Cold War era.

Notes

[8] Boyd, John R., *A Discourse of Winning and Losing*, Air University, Maxwell AFB, AL, 1987), pg. 214.
[9] *Commission on the Roles and Capabilities of the United States Intelligence Community* (the Brown Commission), U.S. Government Printing Office, 1 March 1996.
[10] Kuehl, Dan, *What's New About Information Warfare?*, NDU Press, 21 Mar 97, pg 10.
[11] Von Clausewitz, Carl, *On War*, Princeton University Press, 1984, pg 110.

Notes

[12] Griffith, Samuel, *Sun Tzu, The Art of War*, Oxford University Press, New York, NY, 1971, pg 77.
[13] Clausewitz, pg 75.
[14] Kuehl, pg. 9.
[15] DoD Directive 3600.1, *Information Warfare.*
[16] General Accounting Office (GAO), *GAO Executive Report - B-266140*, Report to the Committee on Governmental Affairs, U.S. Senate, May 22, 1996, pg 3.
[17] Barry, John A., *Technobabble*, MIT Press, Cambridge, MA, 1992; Baker, Russell, *A Little Cyber Grouch*, New York Times, March 25, 1995, pg. 15.
[18] The current Air Force definition of *information warfare* is: "Any action to deny, exploit, corrupt, or destroy the adversary's information and its functions; protecting ourselves against those actions; and exploiting our own information operations." AFDD 2-5, *Information Operations*, 30 September 2001, pg 2.
[19] For other views on the term "information warfare" see Libicki, Martin C., *What is Information Warfare?*, Strategic Forum, Institute for National Strategic Studies, National Defense University, May 1995.
[20] General Accounting Office (GAO), *GAO Executive Report - B-266140*, Report to the Committee on Governmental Affairs, U.S. Senate, May 22, 1996. The attack occurred on March 28, 1994, when computer systems administrators at Rome Air Development Center, Griffiss Air Force Base in New York discovered a "sniffer" program covertly installed on one of their systems. Rome Laboratory is one of four Air Force "super" laboratories and a national center for the development of new technologies for command, control, communications, computers and intelligence (C4I). The initial investigation showed that two unknown individuals electronically penetrated several systems, gained access to all the information residing on those systems, copied sensitive, but unclassified, battlefield simulation program data, and read, copied, and deleted users email messages. Further investigation showed that all of the 30 systems at Rome Labs had been infiltrated and were then used as a springboard to access and gather information from other military, government, academic, commercial systems, and even some foreign military systems.
[21] Molander, Roger C. and Peter A. Wilson, David A. Mussington, Richard F. Mesic, *Strategic Warfare Rising*, National Defense Research Institute, RAND, Santa Monica, CA, Executive Summary, pg. xiii
[22] Esmond, Lt. Gen. Marvin R., Deputy Chief of Staff, Air & Space Operations, Department of the Air Force in minutes of H.A.S.C. No. 106–29, *Lessons Learned From The Kosovo Conflict—The Effect Of The Operation On Both Deployed/Non-Deployed Forces And On Future Modernization Plans*, Hearing Before the Military Procurement Subcommittee of the Committee on Armed Services House of Representatives, October 19, 1999, pg. 15.

Chapter 2

Some Parallels

It is clear that the information age has generated new relationships and greatly expanded the range of possible interactions. It is no longer possible to separate and isolate military, national, public, and private systems. Thus, concepts of national security, to include protecting information systems and deterring attacks, need to be expanded to consider the full range of likely interactions. This would help to determine where the boundary between DoD and the rest of the national information infrastructure should lie. It is in this context that this monograph will address the relationship between information warfare and deterrence.

At the abstract level, the interface between these two concepts is dependent on setting the context clearly. First, deterrence is always from an actor toward a target. The very nature of the actor and target, as well as the degree of asymmetry between them is important. A nation state has much greater power than an individual hacker. A nation state has broad powers of law enforcement that can be brought to bear if the individual is within its borders or the reach of accepted international laws. However, two nation states are, at least in legal terms, equal and must exercise the international system (diplomacy, warfare, etc.) to influence one another's behavior.

Moreover, the nature of the relationship between the states is important to the analysis. The use of deterrence is unlikely in cooperative arrangements, more likely in competitive ones, and most likely in conflict patterns. Finally, substantive context may also make a difference, for example, deterrence is most likely in military arenas where the credibility of threats is greatest and easiest to assess. Hence, specification of the context (type of relationship, nature of the

actors, substantive domain) is essential before any conclusion is possible about the effectiveness of deterrence.

Not unlike nuclear weapons, a weapon of mass destruction, one can draw some parallels between nuclear weapon and information warfare terminology. There are similarities when examining the history of nuclear weapons, as policymakers and military leaders struggled to define the roles and missions for nuclear weapons. There is a similar struggle seen today with respect to information warfare. In fact, policymakers are reluctant, if not completely reticent, to use information warfare offensively. This is a position not unlike the U.S. policy regarding the use of nuclear weapons. What are these parallels of terminology? If nuclear weapons are, in the physical sense, weapons of mass destruction, then one can point to information warfare capable of the same, though not so much in a the physical sense, effects—that is a weapon of mass disruption? An examination of the terminology should identify, if any, these parallels.

Deterrence

On one level, deterrence and information warfare are well matched. Both belong to the world of robust ideas with broad implications. Both are highly relevant to the post-Cold War era in which conflict has been transformed from bipolar global structures to multi-sided, local and regional contests. Still the military element is a crucial part of, but not the driving force for, competition and conflict. Conversely, the two topics can be seen as orders of magnitude apart. Information warfare is a huge domain, ranging from media wars to electronic combat and from economic competition to strategic conflict waged against civilian populations. Deterrence is actually a narrow topic that only applies when a set of quite restrictive assumptions apply. Therefore, the relationship between the two concepts tends to be spotty, highly relevant on some topics, marginally so on others, and not at all relevant in many areas.

Military capability or force is obviously not the only way to deter. For example, economic self-interests may deter just as an employee is restrained from insulting his boss or a salesman from annoying his customer. Nations may be restrained from some information ventures either by the direct cost of the venture or by the harm to future trade and other economic activity that may result. Building economic interdependency can therefore be considered a form of deterrence. Similarly, information actions and interdependency is form of deterrence.

In any area of interest, the retaliatory capability needs not be real, but it must be perceived as real. Conversely, capability to deter may be insufficient if the adversary is unaware of the capability or is not persuaded that the capability might be used. Military examples include the Strategic Defense Initiative as deterrence through perception management. The reverse would include the reality that U.S. military might did not deter Iraq's 1990 invasion of Kuwait. In that case, Saddam Husayn either underestimated U.S. power or its willingness to use that power.

In terms of power, weapons of mass destruction may not serve rational ends. They negate the principle of life itself and cannot serve as instruments of policy anymore. Are weapons of mass destruction able to deter the outbreak of hostilities? Strategic analyst Bernard Brodie thought so when he wrote: "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them."[23] The idea that Brodie expressed was that nuclear deterrence and that nuclear weapons should serve the purpose to prevent their use. Nuclear deterrence is the threat to retaliate with nuclear weapons. In general, deterrence refers to the attempt to create risks that lead the opponent to not engage in a certain policy or action. For deterrence to work the risk must be disproportionately higher than any

possible gain. For nuclear deterrence to succeed certain physical and psychological preconditions have to be satisfied.

For deterrence to succeed, a threatening nation has to be capable and willing to use its nuclear weapons and must effectively communicate this to the nation that is to be deterred. To be effective, several conditions must be met. A deterrent force must be capable to inflict unacceptable damage, or more precisely the threatening nation has to be capable to exact payments (at a cost acceptable to itself) either by denying the opponent to achieve the objectives, by charging the opponent an excessive price for achieving it, or by a combination of the two. There must be no way for the opponent to eliminate the deterrent capability of the threatening nation. The threatening nation must have the plans and the readiness necessary to demonstrate that it can deliver on its "message." Conveying willingness to use retaliatory forces creates a dilemma because the threatening nation must show willingness to engage in a war it tries to deter or prevent.

In addition, the threatening nation must successfully communicate to the opponent the price it will have to pay for attempting to achieve an unacceptable objective. For the U.S. conveyance of the deterrent message had two features in that deterrence had to address foe as well as friend. The opponent had to believe in deterrence. The deterrent message must have some degree of credibility. Both nations must believe that there is a real probability that the threatening nation will indeed perform the promised action, if required.

The components of nuclear deterrence had a physical and a psychological character. On the physical level, deterrence required a series of military instruments, sufficient to threaten the opponent in a way that it would not even think of attacking. Successful deterrence was guaranteed only if there was the will to use these weapons. Deterrence is credible only if a

nation is able to successfully convey the first two points to it's opponent, that it is capable and willing. In other words, successful deterrence depends on psychological components: communication and perception.

This is as true for information warfare as it is for nuclear weapons. Information warfare differs little from traditional nuclear or conventional warfare in developing deterrence strategies. Both forms of conflict are dominated by a strategic dynamic driven by the presence of contestable deterrent costs. Deterrence is fluid, in constant need of maintenance, and in the end prone to possible occasional breakdown. When applied to the concept of information warfare, the utility of a deterrence model and the practicality of a deterrence strategy seem even more useful as information warfare focuses on societal connectivity, which can be attacked, disrupted, or destroyed on three different levels: the personal, the institutional, and the national—not unlike nuclear weapons.

Containment

The term containment describes the foreign policy strategy pursued by the U.S. after the World War II. George F. Kennan, a diplomat and U.S. State Department adviser on Soviet affairs, introduced the term into the public debate. In his famous anonymous X-article Kennan suggested a "long-term, patient but firm and vigilant containment of Russian expansive tendencies."[24] The strategy of containment found its first application in the Truman Doctrine, which guaranteed immediate economic and military aid to Greece and Turkey. John Lewis Gaddis argued that all post-1945 U.S. foreign policy doctrines and concepts were in some way "strategies of containment."

For Kennan containment was a political concept. As a strategy, containment sought to achieve three goals:

(1) The restoration of the balance of power in Europe.
(2) The curtailment of Soviet power projection.
(3) The modification of the Soviet conception of international relations.

These are shown in Table 1 compared to what the actual applications were. Containment also included the creation of military alliances such as NATO, forward basing for forces abroad, extending the "nuclear umbrella" to U.S. allies, and sharing military technologies.

Goals	Means (Kennan)	Actual application
Restoration of the balance of power	Encouragement of self-confidence in nations threatened by Soviet expansionism	Long-term program of U.S. economic assistance (Marshall Aid)
Reduction of Soviet ability to project power outside	Exploitation of tensions in international communism	Cooperation with communist regimes; supporting Titoism in Yugoslavia
Modification of the Soviet concept of international relations	Negotiating settlement of outstanding differences	Using carrots and sticks; containing Germany with an embrace and Russia at arms length

Table 1. Containment Goals

Given the goals, reflecting a unipolar environment, can information warfare accomplish the same? Can countries be just as effectively contained? Within an "information umbrella" and within military alliances? Yes, but there are technology differences among our allies and coalition partners that may impair effective information operations. Here the term containment finds a similar use when discussing information warfare where its deterrence capabilities can be used to achieve national goals/interests.

Flexible Response

Flexible response is the threat to use any, or all, response options to destroy adversary capabilities through a sequence of conventional and nuclear response options. Flexible response was developed to link conventional and nuclear forces. Unfortunately flexible response was no

highly explicit theory nor written in a single authoritative source. It was realistic in that nuclear weapons couldn't be used and it tried to provide credible means to match non-nuclear escalation. The word "flexible" stressed the value of having "multiple options" available should a crises arise. Having multiple options during a crisis appeared to be better than reference to a few preset war scenarios. Having multiple options was thought to enhance the credibility of the U.S. deterrent, reassuring allies while deterring the opponent. At the same time, however, flexibility made it also improbable that the U.S. would want or need nuclear attack.

President Kennedy wanted to deter all wars, general or limited, nuclear or conventional, large or small. Eisenhower and Dulles had wanted to achieve similar goals at minimal cost but their risk was to either not act at all or respond at all levels of threat beyond the original provocation. Kennedy disregarded costs and emphasized sufficient flexibility to avoid the alternatives of either escalation or humiliation. In particular Kennedy wanted to increase the range of available options prior to resort to nuclear war. The threshold beyond which the President might have to decide to initiate the use of nuclear weapons had to be raised. Also, the damage caused by a war with tactical nuclear weapons seemed too high. Moreover, a continued reliance on nuclear weapons could lead to their further proliferation. The basic idea of flexible response, however, was to increase the ability to confine the response to non-nuclear weapons. The ultimate success of “flexible response” was the credible threat to use nuclear weapons, along with the demonstrated capability to use such weapons.

Information warfare offers numerous tools and methods from mass disruption to precision strike such that one would want to maintain multiple options for crises as they arise, enhancing the credibility of its deterrence. Given the multiple options, such flexibility in information warfare tends to make its use improbable. No one option can be explicitly defined

in terms of disruption, denial, degradation, or destruction. In fact, networks offer myriad outcomes of n^{th} order effects that are difficult to predict with any high degree of certainty. Defense against such attacks would require high expenditures of time, resources, and manpower. Therein lies deterrence when faced with an adversary that can effectively attack one's information networks. Again, to be credible, the threat of use must be perceived as real and demonstrated. The use of computer viruses and other software measures has become a fact of daily life on networks across the globe. However, a more effective demonstration would be similar to "This is a Test" detailed in the introduction of this monograph.

Counterforce/Countervalue

Targets described as countervalue are essentially those things that people value the most such as their lives and their homes, and counterforce refers to military capability, especially the fielded forces. Debates of countervalue and counterforce strategies occurred as a notional differentiation of nuclear targeting. Countervalue and counterforce strategies targets were divided into two categories:

(1) Countervalue strategy targets the military-industrial infrastructure and cities.
(2) Counterforce strategy targets the opponent's fielded forces

The idea was that counterforce targeting could give the adversary the incentive to not strike U.S. populated cities. Countervalue, considered the true deterrent, would be accomplished with a secure and guaranteed second-strike of mutually assured destruction. In combination with the strategic Triad, different strategic forces were assigned different targeting options and objectives. Ultimately, policymakers came to think that deterring an attack was more important than limiting the damage and destruction. In information warfare, targeting would meet same definitions.

Massive Retaliation/Mutually Assured Destruction

Massive retaliation was an all-or-nothing strategy. It was the threat to turn the adversary into a smoking, radiating ruin at the end of two hours. By making nuclear war too destructive by making the distinction between victor and loser in such a conflict increasingly meaningless, the deterrent strategy was aimed at eliminating war itself. Furthermore, massive retaliation meant the possible deterrence of an all-out attack. Massive retaliation reflected a policy of "brinkmanship." The expectation was that by going to the "brink of war" the U.S. would be able to deter future challenges like Korea.

It turned out that the threat of massive retaliation could not prevent limited challenges. It was not an effective foreign policy tool to deal with everyday problems. Short of an ultimate provocation, an adversary could raise tensions and challenge the U.S. as the Soviet Union did in the Korean War. In other words, more limited responses were necessary to deal with less-than-total challenges. When the Soviet Union achieved nuclear parity with the U.S., the Cold War entered a new phase. The cold war became a conflict more dangerous and unmanageable than anything the U.S. had faced before. Many would argue that world stability and deterrence was actually made possible because of the existing duopoly (U.S. vs. USSR) and that world stability today is more difficult to maintain in a monopolar world

In the early cold war years, the U.S. had enjoyed superior nuclear force, an unchallenged economy, strong alliances, and a trusted President to direct his incredible power against the Soviets. In the later years of the cold war, however, Soviet forces achieved nuclear equality whereby each side could destroy the other many times. This fact was officially accepted in a military doctrine known as Mutual Assured Destruction (MAD). MAD began to emerge at the end of the Kennedy administration and reflected the idea that one's population could best be protected by leaving it vulnerable so long as the other side faced comparable vulnerabilities. In

short, whoever shoots first, dies second. Today, information warfare offers same capability against advanced societies, but would be problematic towards less developed societies.

A Comparison

Having laid the basis and background for U.S. nuclear strategies, a summary of the similarities of strategy as applied to information warfare is given. Deterrence is defined as:

- A threat to something of value that exceeds the perceived gain of non-compliance.
- A clear statement of the behavior to be avoided or performed.
- Clear and unambiguous communication of the threat and the desired or proscribed behavior to the target.
- Credible threat, meaning that the actor is perceived by the target to have the will and capability to execute the threat.
- Situational constraints that make it impossible for the target to avoid punishment.
- Controllability of the threat and its implications by the actor.

Thus the deterrent use of force is intended to prevent an adversary from initiating an action by threat of unacceptable retaliation. The effectiveness of the threat, credibility, depends on an actor's ability to convince a potential adversary that it has both the will and capability to punish the potential antagonist severely if the undesirable action is carried out. Certain preparations such as protecting targets may both reinforce deterrence through reducing an adversary's perceived ability to prevail in a conflict while also strengthening one's defensive ability to minimize the damages if an attack does occur. Both active defense and passive defense should leverage the overall deterrent effect.

In information warfare, it differs little from traditional nuclear or conventional warfare in developing deterrence strategies. Both forms of conflict are dominated by a strategic dynamic driven by the presence of contestable deterrent costs. Deterrence is, therefore, fluid, in constant need of maintenance, and ultimately prone to occasional breakdown. When applied to the information warfare, the utility of a deterrence model and the practicality of a deterrence strategy seem even more useful as information warfare focuses on societal connectivity, which can be

attacked, disrupted, or destroyed on three different levels: the personal, the institutional, and the national—not unlike nuclear weapons.

Containment denoted measures to prevent further enlargement of the Soviet bloc (and its nuclear arsenal), which, the U.S. feared, might gain hegemony and pose the gravest dangers to other nations not only in Eurasia but also in the U.S. if allowed to grow unchecked. The policy of containment required a new strategic design. As a strategy, containment sought to achieve three goals: the restoration of the balance of power in Europe, the curtailment of Soviet power projection, and the modification of the Soviet conception of international relations. For information warfare the terms find a similar use. In this case, information warfare in terms of its deterrence capabilities could be used to achieve similar national goals/interests, especially against advanced nation states.

Flexible Response called for the continued reliance on sizable conventional forces. Such conventional forces served two functions, a deterrent function and the function to fight limited wars. The basic idea, however, was to increase the ability to confine the response to non-nuclear weapons. The word "flexible" stressed the value of having "multiple options" available should a crises arise. Having multiple options was thought to enhance the credibility of the deterrence (reassuring allies while deterring the opponent). Flexibility also made it improbable that the one would want, or need, nuclear attack. Information warfare offers numerous tools and methods from mass disruption to precision strike that one would want to maintain multiple options for crises as they arise which enhance the credibility of its deterrence. Given the multiple options, such flexibility in information warfare tends to make it problematic (if not high cost, high risk) for one to conduct an information warfare attack when faced with potentially n^{th} order effects.

Counterforce is the targeting of strategic offensive forces against the military and military support capabilities of a nation with an effort to spare adversary population and general industrial resources. Countervalue is the targeting of strategic offensive forces against the industrial and population centers of a potential adversary. These targeting strategies hold the same for information warfare. Mutually assured destruction is that capability of strategic offensive forces to destroy an aggressor nation as a viable society even after surviving a surprise first strike. Information warfare offers same capability against advanced societies, but would be a daunting task against less developed societies.

One could argue that policymakers today treat offensive information warfare in analogous ways to nuclear warfare. Policymakers, and some senior military leaders, are reluctant to use offensive information warfare as this "weapon of mass disruption" can bring reciprocal effects much like a nuclear weapon but with far less physical destruction. Yet, it remains to be seen what the overall effects of offensive information can bring about. Its effects can be lethal or non-lethal. Clearly there would be mass disruption if an attack were made on the New York Stock Exchange that shut down trading altogether. Yet a more sinister form of mass disruption would be to deliberately delay trades by just a few minutes. The question remains: would the "day after" of an information warfare attack bring about as much chaos as could a nuclear weapon?

Information Warfare Weapons

Just as the purpose of war is to destroy an adversary's will and/or capacity to fight, a weapon is a tool that allows one to achieve the objectives. Thus, it is reasonable to assume that an information warfare "weapon" must be able to diminish the adversary's will and/or capacity to fight. Hence, information can be considered a legitimate weapon of war. The obvious

question is to determine whether the use of information can contribute to the purposes of war. If one would say “yes,” then one can conclude information is a weapon. If one would say “no,” then information is not a weapon. In this case, information is and remains a weapon that contributes and leverages the purposes of war.

Information warfare weapons may be even more exotic than computer viruses. Los Alamos National Laboratory in New Mexico has developed a suitcase-size device that generates a high-powered electromagnetic pulse (EMP). Special Forces could sneak into a foreign capital, place the EMP suitcase next to a bank and set it off. The resulting pulse would burn out all electronic components in the building. Other proposals combine biology with electronics. For example, Pentagon officials believe microbes can be bred to eat the electronics and insulating material inside computers just as microorganisms consume trash and oil slicks.

There are new information warfare weapons specifically designed for use in the domain of information systems and networks. New viruses are being created at an incredible rate as well as their countermeasures and anti-viral software. Available now on the market are meta-programming environments that "incubate" viruses in accordance with the desires of the attacker. The variety and combinations are intimidating. Cruise viruses are capable of destroying specific data sets, stealth viruses conceal themselves from detectors and monitors, and polymorphic viruses encrypt themselves using variable keys. There are also new protected mode viruses that have become the standard common file infector and boot sector virus. This class of weapons aims to control or disable the operating logic of the targeted networks and systems. Using the operating systems software, as well as the different utilities, the virus can make the system to act upon data in a different way or even simply waste cycles.

These are just a sample of the weapons that information warfare can bring to the fight. Some can be accurately targeted, like precision-guided munitions, and impact a single target. Others are more like a weapon of mass disruption that impacts total networks, systems, and the very infrastructure of an entire society not unlike the use of a nuclear weapon. The next chapter will examine how these weapons can be used for offensive information warfare.

Notes

[23] Brodie, Bernard, *More about Limited War*, World Politics 10, No. 1, October 1957, pg. 117.
[24] May, Ernest R., *Introduction: NSC 68: The Theory and Politics of Strategy*, Department of Military Studies, Readers: Book 2, Maxwell AFB, AL, 1994, pg. 21.

Chapter 3

Offensive Information Warfare

There are many weapons that information warfare can bring to the fight, ranging from a precision strike on a single target to one of total system wide mass disruption. Offensively one can target a single PC or total networks, systems, and the very infrastructure of an information-dependent society. A useful definition or model of information warfare therefore has to describe the ultimate objective in order to identify and target the applicable elements of information warfare. To better understand the reluctance to use offensive information warfare, one needs to examine the elements of policy, strategy, and the constraints/restraints involved. The concept of information warfare can be broken down into three parts:

(1) A set of IW elements (techniques and capabilities).
(2) A comprehensive strategy that employs them.
(3) A target and objective. Only the elements are common to both IW and the earlier concepts of information attack.

This section will look at the elements of offensive information warfare and examine policymaker's and military leader's reluctance to execute such an offensive.

Policy

Policies for developing and using military forces are formulated by the national political authorities and conveyed to the armed forces through the Secretary of Defense. Few, however, have paid much attention to just how and by whom information warfare forces are to be developed to support national policies. More importantly, what are information warfare forces? Who will use these forces? Who will authorize their use? To what ends? New tools and technologies for communication have created the potential for this new form of warfare to a

degree once imagined only in science fiction. Once one understands what information warfare can do and how it can be used as a weapon, they may be reluctant to use it, again, not unlike nuclear weapons.

The futurists Alvin and Heidi Toffler have argued that the U.S. armed forces need to develop a "systematic, capstone concept of military knowledge strategy;" where such a strategy would include clear doctrine, and a policy for how the armed forces will acquire, process, distribute, and project knowledge.[25] The strategic use of information warfare presents a broad and complex spectrum of issues and challenges to existing decision-making processes. Thus, it is clear that some sequencing in taking up these issues nationally and internationally would be appropriate. These key strategy and policy issues can be roughly characterized as:

1. **Easily implemented.** Those issues that could be moved to closure nationally (and, in some cases, internationally) without undue difficulty once suitable processes are identified or established. Who should have the lead responsibility? The government (and, if so, who within the government) and/or industry (and, if so, who within the key infrastructures) in the U.S. national response to the information warfare threat? These lead to different choices to where the U.S. should focus its attention:
    - Federal government leadership with a national security focus.
    - Federal government leadership with a law-enforcement focus (for example, Department of Justice).
    - Joint international government leadership with a national security focus.
    - Joint international government leadership with an law-enforcement focus.
    - International industry leadership with government support.
2. **Warning, attack, and emergency response.** How should the U.S., including its governments and its industry, organize to develop and implement capabilities and

procedures to sense and respond to information warfare threats? Some suggested models are:

- A government-led national security-oriented model or a National Infrastructure Condition (NICON) model.
- A government-led law-enforcement-oriented model or a counter-terrorism model.
- A Centers for Disease Control and Prevention (CDC) model.
- An industry-led model.

3. **Vulnerability assessments.** By what means and mechanisms of government and industry cooperation should a vulnerability assessment of key U.S. national infrastructures be undertaken? Possibilities include:

   - A government-led, or DoD-led, assessment of U.S. vulnerabilities.
   - A joint public and private sector effort involving the U.S. and other key nations.
   - An international public-private partnership, such as the CDC and the World Health Organization (WHO).
   - An industry-led and government-assisted assessment.

4. **Declaratory policy on offensive IW use.** What should U.S. government declaratory policy be on the use of offensive information warfare and its relationship to use of other strategic military and economic instruments? What should be publicly declared versus one's classified capabilities? This policy should include:

   - Retaliation principally in kind for any information warfare attack.
   - Retaliation principally by non-information warfare military means in response.
   - Retaliation by economic means, including economically oriented offensive information warfare means, in response.
   - Complete ambiguity as to how the U.S. would respond to such an attack and prepare for preemptive information warfare.

Such policy issues will require serious thought and collaborative efforts to implement. The U.S. needs to have a well-developed warning, attack, and response system that mitigates the effects of an information warfare attack. Further, a thorough analysis of key U.S. infrastructure should

delineate critical vulnerabilities and offer workable solutions that minimize these vulnerabilities. Finally, the U.S. must determine what are its best response options to information attacks.

Issues

There are urgent but contentious issues related to the initial charting of long-term and strategic information warfare (SIW) related national goals and strategy. Some of these issues include:

- **Research and development (R&D) investment strategy.** What investment strategy should the U.S. pursue for:
    - Monitoring, perpetrator identification and "trackback" techniques.
    - Attack assessment techniques.
    - Defense and reconstitution techniques.
    - Damage assessment techniques.
- **International information sharing and cooperation strategy**. What principles should guide international collaboration, in particular with allies and coalition partners, in the information warfare domain? It has been shown that there is a parallel for deterrence and information warfare. Thus a strategy of cooperation could include:
    - National security-oriented network protection goals.
    - Coordinated defensive R&D with allies.
    - International proscriptions on offensive SIW R&D.
    - Private sector or market-driven focus.

Clearly the U.S. must develop an investment strategy for future advancement of information warfare offensive and defensive techniques. Once these are developed, the next step is to determine how much should the U.S. share its information warfare systems and techniques with its allies and coalition partners. Should the U.S. bring its partners under an information warfare umbrella similar to the nuclear umbrella it shared with NATO?

There are many issues that have been deferred because of technical uncertainties to be taken to closure. Worse, some issues that are taken to closure hastily, possibly producing a "bad" strategy or policy decisions, would be hard to reverse. These issues are intertwined within the policy and strategy realms that include:

- **Intragovernmental and intergovernmental cooperation on politically sensitive privacy issues.** This needs to be included in any discussion of information warfare. How will privacy rights be protected under specific strategies and policies?
- **Minimum essential information infrastructure (MEII).** More analytical and conceptual work is needed to determine whether the MEII issues and concepts are at all feasible from both a technical and cost standpoint.[26]
- **Encryption policy.** Information warfare is just one of the many areas that need to be discussed when the U.S. and the international community chart long-term encryption-related goals and strategies.

Each of these issues requires sensitive treatment. In turn, each of them overlaps with other elements of a comprehensive approach to addressing offensive information warfare policy and strategy concerns. The notion that an action plan for addressing information warfare vulnerabilities requires that tradeoffs be made among different factors is central to the unprecedented uncertainties of the information warfare environment

Strategy

Strategy, according to the DoD, is the "art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat."[27] For most people, it is obvious that the political and economic aspects of the national security policies of the U.S. are developed by the national political authorities (e.g., the president and the Congress) and, in dealing with foreign states or groups, executed by the Departments of State, Commerce, Agriculture, etc.

Given the myriad of issues facing policymakers with respect to offensive information warfare, one must understand the strategic nature of warfare; that is, strategic information warfare. For ease of understanding, this relationship with respect to other weapons the warfighter brings to the fight is shown below:

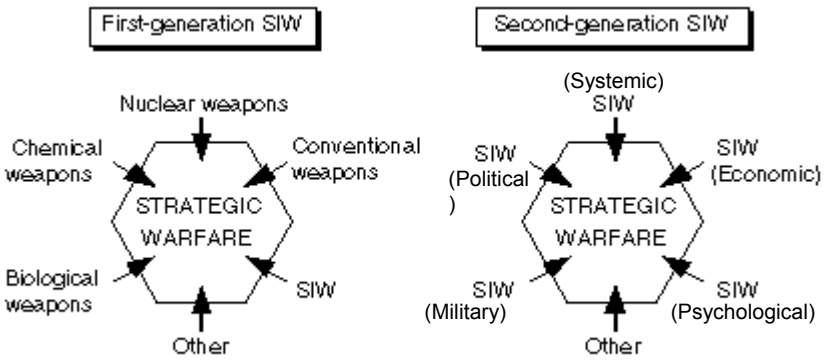

Figure 2. Two Concepts of Strategic Information Warfare[28]

Using figure 2, SIW might be conceptualized in the following terms:

1. **First-Generation SIW.** SIW as one of several components of future strategic warfare broadly conceptualized as being organized through a number of strategic warfare instruments.
2. **Second-Generation SIW.** SIW as a separate, fundamentally new type of strategic warfare generated by the information revolution, implemented in newly prominent strategic warfare arenas (e.g. economic) and on time lines (e.g. years versus days, weeks, or months) than those generally attributed to strategic warfare.

U.S. decision makers use force only reluctantly. When called for, they prefer to apply it massively so as to minimize friendly casualties, collateral damage, and terminate hostilities as soon as possible. To that end, political and military objectives should be clearly stated so that progress toward them can be monitored so that it will be evident when they have been achieved. Targets must be selected carefully e.g. noncombatants must not be targeted directly, and religious shrines, works of art, monuments, and the like must be preserved. Collateral damage must be minimized. Moreover, unintended consequences are to be, as much as possible, ruled

out and fratricide must be avoided. In fact, it is desirable that casualties on both sides be minimized.

By this code, a preemptive attack by U.S. armed forces is desirable and workable at the tactical level of warfare. But such an attack is problematical at the operational level, and unlikely at the strategic. That is, the U.S. goes to war only when forced to do so, but once engaged acts swiftly, aggressively, and decisively. But it has been loath to preempt. Because of this greater reluctance to preempt at the strategic level, the U.S. is more vulnerable to strategic surprise and its detrimental effects. Yet if information warfare is not considered to involve the use of force, preemption by such means might well be undertaken at any level. If information warfare can be distinguished from the use of force, then the traditional U.S. inhibition about initiating hostile action, especially at the strategic level, is no longer relevant.

Because information warfare can take place at very high speeds and without warning, the implications of surprise are potentially serious at all levels of warfare. If this distinction about the operational acceptability of information warfare is recognized, U.S. decision makers must assess the possibilities for the adversary to retaliate, and they must determine whether they can defend against or tolerate that retaliation. If they cannot, the U.S. will probably be dissuaded from attacking.

While these seem like a set of operational constraints without objection or exception, they are actually unique. Most of them are clearly of minimal concern to potential U.S. opponents, with respect to their own acts. One that is of interest to opponents, however, is the last one: assessing the potential for the adversary to retaliate. If deterrence by threat of punishment has a hinge, this is it. Still, by the operational restrictions the U.S. places on itself, the question of retaliation is made an issue. That is, with regard to punishment, the certainty of retaliation is what deters.

Deterrence is weakened to the extent that an adversary is uncertain about the level of retaliation or whether it will occur at all. That is not a matter only of capability but also of "will" to retaliate. It is a particularly difficult task for information warfare to convince a potential adversary that one has the will to retaliate with offensive information warfare and that the adversary will be much worse off because of that retaliation.

In information warfare, as in terrorism, the possibility exists that a devastating attack will be made without the perpetrator being identified. The difficulty of determining the source of computer hacking or the origin of a virus gives rise to concern about catching a culprit or retaliating against an attacker. Even if an attacker can be identified, questions arise about the proper form of retaliatory action. Such questions weaken deterrence by reducing the certainty of retaliation. If one can formulate no appropriate and effective form of retaliation, one is left to rely on deterrence by denial. Thus strategy and policy are interlinked and are dependent upon each other when, and if, one should determine to use offensive information warfare.

Constraints/Restraints

Where is the line drawn between non-lethal and lethal (n^{th} order) effects? A significant body of legal restrictions on the use of force has been formalized that resides in international law, in particular in the Law of Armed Conflict, and in arms control agreements, which are legally binding documents. The law differentiates between initiating the use of force, *jus ad bellum*, and how force is used in war, *jus in bello*. To satisfy the law, the use of force must stem from a cause that is just, be motivated by right intentions, and be authorized by competent authority. In addition, four tests must also be passed:

(1) The use of force must have a reasonable chance of success.
(2) It must be expected to produce a net balance of good over evil.

(3) It must be a last resort.
(4) Peace must be the expected outcome.

The Charter of the United Nations, moreover, takes *jus ad bellum* another step, requiring that the use of force always and exclusively be in self-defense.

Once warfare has commenced, whether or not the requirements of *jus ad bellum* have been satisfied, different criteria must be met which are necessity, proportionality, discrimination, and humanity. The Law of Armed Conflict has provided specificity to the requirements of *jus in bello*. These deal, among other things, with the rights and responsibilities of belligerents and neutrals and with the protection of noncombatants in time of war. For their part, arms control constraints limit quantitatively and qualitatively the inventories and deployment of armament. There have been no specific arms control agreements directed at limiting information warfare. In fact, however, with its emphasis on confidence-building measures and operational transparency, arms control has acted to hobble effective information warfare.

Other treaties and executive agreements have a potential effect on information warfare as well. The International Telecommunications Satellite Organization (INTELSAT) Agreement of 1973, for example, seeks to ensure that satellites are used only for peaceful purposes.[29] While the agreement does recognize satellite systems with military purposes and exempts them, the DoD uses civilian systems heavily.[30] Whether information warfare activities that involve such systems, including portions of the Internet, are always to be regarded as "non-peaceful" is a fundamental legal issue that has not yet been resolved.

Similarly, federal law governs covert and clandestine acts under the mantle of national security require Presidential finding and Congressional approval. A variety of peacetime information warfare defensive activities might fall within this category, especially those involving emplacement of information operation "agents," but this too has not been determined.

Over and above operational, organizational, and legal constraints, there are moral considerations. U.S. foreign policy has always had a moral element that asks whether the nation may undertake a particular act or follow a certain policy line that is legally permitted and prudentially attractive. U.S. decision makers are often torn by competing requirements, such as the need for humanitarian intervention and the principle of noninterference with internal affairs of other states. It is even difficult even to articulate a moral code in such circumstances, let alone that the U.S. follow one consistently.

Among these vexing issues is separating intellectually the use of force or information warfare among nation-states from that in the context of interpersonal relations. International actions often are judged indiscriminately under the same set of rules and with the same moral template, as are interpersonal situations. Yet the actions a state may morally and legally do are very different from those that individuals or non-states may do. Dean Acheson articulated the difference over thirty years ago: "A good deal of trouble comes from the anthropomorphic urge to regard nations as individuals. . . . The fact is that nations are not individuals; the cause and effect of their actions are wholly different."[31]

U.S. decision makers believe it is important for the nation to act as a moral leader in interstate relations. One consequence of this view is that policies or actions should not cause unnecessary suffering on the part of noncombatants in a target state. Moreover, the U.S. is uncomfortable with the notion of superiority, believing strongly in equality and human rights. This makes it somewhat awkward for the U.S. to deliver a deterrent threat based on superior capabilities. Public justification of the use of information warfare will be important because the moral aspects of U.S. policy will demand it. How the use of information warfare is morally justified will go a long way toward determining its roles relating to the use of force. The

difficulty is defining when is using information warfare considered the use of force? Clearly, not all information warfare meets the definition but it does have the capacity to disrupt, degrade, deny, or destroy much like other weapons of force. The distinction between information destruction by a disgruntled employee or an actual planned information warfare attack is blurred. One is a criminal act, the other could be considered an act of war.

As a result of the interplay of these factors, the ability of the U.S. to deter an information warfare attack can be assessed as no better than full of twists and turns. The capability of this nation to respond to an information attack by a state or an organized, locatable group (such as terrorists) cannot be doubted, but its will to do so is another question. If the attacker is adaptable and hidden, the U.S. will have to rely on deterrence by denial. This precludes the harms that a determined and competent information attacker may seek to cause, or acting in such a manner that even successful attacks prove to be of no benefit to their perpetrator. Unfortunately, self-protection is a key aspect of deterrence by denial, and that is another weak point in U.S. information warfare.

Deterrence by both punishment and denial could be bolstered by communication of a deterrent policy and other actions that communicate the willingness of the U.S. to play an active role in information operations across the board. As the Defense Science Board concluded, "Deterrence must include an expression of national will as expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack."[32]

The Commander and ROE

Information warfare weapons must meet the same tests for necessity and proportionality as other weapons under the laws of armed conflict. In addition, commanders must recognize and weigh the possible consequences of weapons that can devastate the information systems of an adversary. The commander contemplating the use of information weapons must consider problems such as lack of adversary command-and-control, collateral damage, post-hostility reconstruction, and retaliation, among others. Because of the extraordinary disrupting consequences of these weapons, there must be guidance for their employment, and commanders must carefully consider adverse effects from their use.

The term "information warfare" has thus caught the attention of an entire generation of military thinkers. While the term encompasses both offensive and defensive measures, much of the imaginative thinking has concerned attacks on an adversary's command-and-control and information systems using methods as diverse as computer viruses, laser beams, or high-powered microwaves. Much of this thought goes into understanding the possibilities and maximizing the effects of high technology in information warfare. For example, imagine what the consequences would be if the following systems were targeted and disabled: financial markets, nuclear power plants, telephone systems, power distribution systems, traffic lights, railroads, energy grids, pagers and cell phones, communication lines, water distribution systems, or air traffic control and airline reservations systems.[33] This is tantamount to a weapon of mass disruption, a key characteristic of an all out information warfare attack.

The ability to destroy precisely and completely the adversary's command-and-control system, and the ability to attack his information infrastructure, requires the operational commander to carefully ask new questions. The question of "what can I do" with information weapons already has a litany of answers, and will find no shortage of further ones in the near

future. Perhaps the more important question, and one that is only recently receiving the attention it deserves, is: "when shouldn't I use" these high-technology weapons?

If there is something that one can learn from the past about new weapons or methods of warfare, it is that they will often encounter unforeseen limitations in their use. Chemical weapons were so lethal and indiscriminate as to be banned and nuclear weapons were so powerful that their use became almost unthinkable. The weapons of information warfare have effects as potentially devastating as those of nuclear weapons, yet there has been relatively little resolution in the debates on the implications of the newest technologies and their use in warfare. There are legal and practical limitations that the President, SECDEF and, more importantly, the operational commander, must consider before employing these technologies.

Some may argue that non-lethal forms of information warfare, such as compromise of an adversary computer system, do not constitute the "use of force," and therefore are not subject to the laws of armed conflict. To advance that debate, proponents must instead show that these actions are legal under peacetime international laws, which is a tremendous task. U.S. government officials, for example, have reportedly rejected intrusion into other countries' computers, considering them to be a "fundamental attack." Clearly, international law would consider such acts illegal in peacetime. Therefore, these intrusions must be measured against the principles of the laws of warfare.

What then are the minimum levels of command-and-control that the operational commander must allow an adversary to maintain while rendering him ineffective? A perfectly executed command-and-control warfare attack would decapitate the adversary leadership with no means to communicate with his forces. There are several reasons, however, why this might not be the ideal situation for the commander. The first is the most obvious. Should the perfect

information warfare campaign leave the adversary command with no means to fight, it would also be unable to communicate its desire for surrender or truce to its troops. Military units are trained to fight autonomously in the event of lost communications, and, until a reliable and believable command to halt hostilities is received from above, they are likely to continue fighting. While a relatively impotent force, like the retreating Iraqi Republican Guard, might cause few problems, it is easy to imagine a situation like the one in the Pacific theater during World War II where capable Japanese units, isolated by complete destruction of their means of communication, continued to fight. Current techniques of jamming can be simply stopped to allow radio communication, but technology such as an electromagnetic pulse could ruin all communications equipment in a large area.

Another consideration is the link between an adversary's information flow and the commander's attempts at military deception. While deception may be aided by degraded communications, severely deteriorated information flow may instead negate attempts at military deception. Often the desired end of the deception plan is not simply to prevent the adversary from gaining knowledge of an operation, but to cause him to distribute his forces unwisely, and to his disadvantage. For example, the German insistence that Patton would soon be crossing the Channel made the D-Day invasion a success. Had the Germans not had any information at all about the disposition of forces in England, they may have reacted immediately to the D-Day forces by moving reserves down the French coast to oppose it. Therefore, the commander must ensure that his attempts at deception are not obstructed by successful information warfare.

In terms of economy of scale, selective and subtle forms of data manipulation may prove more of an impediment to the adversary in the long run than overt destruction. An adversary intelligence system, for example, is more valuable as a source of misinformation than it would be

as a target of destruction. It is the principle of the double agent, and the reason such spies are "turned" rather than exposed. The commander is obligated to assess the possibilities of exploiting an information resource before he authorizes its destruction.

Consider the situation where a belligerent has infiltrated an adversary logistical database. If the database is dual-use (military and civilian), legal questions could prevent widespread destruction of data. But even with a purely military system, complete destruction of a logistical tracking system, while certainly legal, would alert the adversary of the attack, and prompt him to take countermeasures such as "hardening" the system or restoring the data. However, selective use of data manipulation could divert vital material at a critical time away from the war effort and still go undetected. In the long run, this technique might not only prove more justifiable but also more effective. However, even data manipulation may be unsuitable. Warren Caldwell, a Naval War College faculty member, wrote that information warfare "may be an unsuitable or inappropriate means to deal with prevalent forms of conflict in the new world order."[34] His comment questions the efficiency of information warfare and notes that information technology may not live up to its promise.

One prevalent characteristic of modern conflict is a trend toward multinational coalitions. The U.S. has developed this trend to include multinational headquarters, intelligence centers, operations centers, and command structures. Commanders will be required to consider the problems of technology transfer and capability exposure during such operations. Problems of technology transfer may limit the scope of information weapons they can employ.[35] A similar problem arises for the commander during a conflict against a relatively minor adversary. Some of these information warfare weapons are so advanced that potential opponents may be unaware of their existence, and their use may provide future adversaries advance warning. Like the

ongoing rush to counter stealth technologies due to Persian Gulf War successes, a single use of an information warfare technique could engender countermeasure development that may render it ineffective in future, more critical contingencies.

Another trend in recent conflicts is the involvement of "non-legitimate" adversaries, either because the current government had become corrupt (e.g. Panama, Haiti), or because the adversary was working outside the bounds of the legitimate government (e.g. drug cartels, Al Qaeda). In these cases, attack on legitimate military targets may cause serious problems for the legitimate government. The use of information warfare in infiltrating and isolating drug money in Colombian or third country banking systems is a good example. This action could have adverse effects on the credibility and stability of the targeted financial systems. Legitimate investors may have second thoughts on using systems that have been penetrated, or the damage to those systems could prevent their legal use.

A final problem for the commander to consider, especially with new, highly destructive technology, is the problem of retaliation. The U.S. is the most information-dependent country in the world, and, even if military systems are hardened, has the greatest vulnerability to information attack. As Time magazine says, "An infowar arms race could be one the U.S. would lose because it is already vulnerable to such attacks."[36] Such attacks could take the form of escalation, or simple desperation. Just as Iraq launched Scud missiles in frustration during the Persian Gulf War, an adversary that found its information weapons ineffective against U.S. armed forces may direct them against civilian targets through the Internet, communication satellites, or undersea fiber optic cables. However, attacks through the Internet can adversely impact military communications for the reason that 70% of military communications employ commercial systems and exploit the military dependence on the Internet. While these targets

may not be militarily significant during actual hostilities, they could prove politically sensitive or at least very disruptive. Intelligence should be tasked to determine possible adversary responses to information attack, and the impact of possible retaliation considered in the selection or rejection of information weapons. Additionally, policymakers and commanders will have to determine, and agree on, what the information threshold or "trigger" will be that evokes an offensive information warfare attack, or even a response.

A Different Look

There are two stages in any major technological advance. The first stage, the current military one for information warfare, is exploratory and inventive. This is the period where new doors are opened, new possibilities glimpsed, and the "explorers" of the era gather their crew in search of new discoveries. In the second stage, the technological limits are found and bounded, untested predictions are tested, and the practical use of new weapons becomes constrained. As it was with nuclear weapons, so it must be with information warfare.

Unfortunately, it's a great responsibility laid upon the U.S. military leaders to walk blindly down the information armory. Choosing and employing new weapons is not without consequences. For them, exploration must be tempered by apprehension. Leaders should, and must, consider with great care the possible consequences of information warfare weapons and the targets selected for compromise or destruction. The greater capacity those weapons have to disrupt, the greater temperance they demand. Military leaders cannot afford to wait until the adversary is at hand before regarding their own arms.

A technique for invading an information system is like a precision guided bomb, in that it can be either legal or illegal in its application. The problem is that the range of illegal possibilities is more difficult for today's commander to comprehend. With any new weapon the

commander is given, he will need explicit guidance in its use, and a discussion of the possible adverse effects. This is even more critical to this new arena of information warfare. A pilot dropping a laser-guided bomb has been trained on the Law of Armed Conflict and the weapon's effects. Commanders, then, must give the same guidance to the computer hacker loading a virus into the financial network of an adversary-or suffer the consequences. Using offensive information warfare involves new weapons, new plans and strategies bounded by national policy. Given the trepidation policymakers exhibit in using offensive information warfare, the threat of use can become deterrent to potential opponents. In the next chapter, information warfare will be examined as a form strategic deterrence.

Notes

[25] Toffler, Alvin & Heidi, *War and Antiwar: Survival at the Dawn of the 21st Century*, Little, Brown & Co., Boston, MA, 1993, pg. 141.
[26] The MEII concept is that system providing a minimal level of communications access and services to critical governmental and societal user communities.
[27] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, pg. 414.
[28] Molander, Executive Summary.
[29] International Telecommunications Satellite Organization (INTELSAT). Established by two international agreements effective in February 1973, INTELSAT promotes the development of the global telecommunications satellite system. In the late 1980s, there were 109 signatory member nations and 30 non-signatory user nations.
[30] U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD 96-84, General Accounting Office, Washington, DC, May 1996; and Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare--Defense (IW-D)*, Office of the Secretary of Defense, Washington, DC, November 1996.
[31] Acheson, Dean, *Ethics in International Relations Today*, Amherst Alumni News, Winter, 1965, pp. 2-3, quoted by James Finn, *Morality and Foreign Policy*, in Michael Cromartie, ed., *Might and Right after the Cold War: Can Foreign Policy Be Moral?,* Ethics and Public Policy Center, Washington, DC, 1993, pg. 38.
[32] Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare--Defense (IW-D),* Office of the Secretary of Defense, Washington, DC, November 1996, Executive Summary, pg. 4.
[33] Sexton.
[34] Caldwell, Warren, Jr., *Promises, Promises*, Proceedings, U.S. Naval Institute, January 1996, pp. 54
[35] Caldwell, pg. 56
[36] Waller, Douglas, *Cyber War,* Time Magazine, 21 August 95, Vol 146, No.8.

Chapter 4

Deterrence—Strategy and Technology

A Military Scenario

First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Then computer logic bombs are set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, adversary field officers obey he orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes, specially outfitted for psychological operations, then jam the adversary's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his computer, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot. [37]

A few years ago, no one took information warfare seriously. But the more one learns about it, the more concerned one becomes.[38] Yet, one can argue, information warfare has been around since at least the fifth century BCE. Information warfare, in the form of code breaking and deception, was powerfully displayed in the World War II, where it was arguably a key to victory in both the European and Pacific theaters, and it played an important role in the Gulf War of 1991. So why do so many people think the U.S. (especially the military) is unfamiliar with information warfare, and why is there such concern about taking it seriously?

Perhaps what is intended is to raise the alarm about some new vulnerability to information warfare that has been exposed in the last few years. These vulnerabilities increase in scope and complexity as societies and economies become more dependent on the free and rapid flow of information. In the U.S. both the General Accounting Office and the Defense Science Board have released detailed reports on the subject.[39] These reports acknowledge that there are problems to be solved, but neither qualifies as a clarion call to urgent action. Even the

President's Commission on Critical Infrastructure Protection identified eight critical domestic infrastructures but produced sweeping statements as to what actions need attention now.[40]

Offensive actions using information operations include those that move information from one place to another, destroy it, propagate disinformation, and corrupt, degrade, interrupt, or deny data flows. Defensive actions seek to protect one's own information from similar actions of an adversary. Clearly, a variety of means can be used in both offensive and defensive information operations. These include the well-known military pillars of command-and-control warfare: electronic warfare, operations security, deception, psychological operations, and physical destruction.[41] Other means include hacker warfare, economic information warfare, and cyberwarfare.[42]

The deterrent use of force is intended to prevent an adversary from initiating an action by threat of unacceptable retaliation. The effectiveness of the threat depends upon the ability to convince a potential adversary that it is both the will and capability to punish the potential aggressor severely if the undesired action is commenced. In peacetime a fundamental U.S. security objective is to prevent war. If conflict should develop, the goal is to terminate it as quickly and with as little damage as possible without compromise of one's vital interests or major objectives. Information warfare can play important roles both in the prevention and the successful prosecution of war. Its effectiveness pivots on its role in deterrence, and on whether it is considered a use of force. For the U.S. military the topics of key interest in information warfare narrow down to two—deterrence and employment.[43]

The tools, techniques and strategy for information warfare will continue to be developed and, during wartime, should be employed. But the resources, organization, and training needed for information warfare will be provided once the national political leadership grasps its war-

winning, and casualty-reducing potential. Such a development would certainly be sensible. On the other hand, many of the tools and techniques of battlefield information warfare can be applied to the strategic level of war. This application would not be prudent, but there are serious reasons to doubt the ability of the U.S. to prosecute information warfare successfully.

One reason is that the U.S. is an open society and it may be too vulnerable to engage in information warfare with an adversary prepared to "fight back."[44] The communications infrastructure, or "information highway," is wide open in U.S. society. The U.S. society may be terribly vulnerable to a strategic information warfare attack. One may find physical control and security to be impossible. The domestic computer, communication, and information networks essential for the daily functioning of U.S. society are very vulnerable to penetration, manipulation, and even destruction by determined hackers.[45] In the future, these may not be amateurs but well paid "network ninjas" inserting the latest French, Iranian, or Chinese virus into part of the Internet.[46] Unfortunately, such attacks via the Internet will rapidly spread through networks and become global with attendant collateral damage. A strategic information warfare attack on U.S. communication systems, including military communication systems, air traffic control system, financial net, fuel pipeline pumping software, and computer-based clock/timing systems, could result in societal paralysis in the form of mass disruption.

At first glance, it is these very capabilities that would seem to pose the greatest threat to the U.S. itself, dependent as it is on an extensive information infrastructure for governance, finance, civil infrastructure, and military effectiveness. Arguably the U.S. has the most extensive system of computer networks in the world; offering plenty of targets to strike; however, that size is also its strength. A network's power increases with its size, thus a larger size equates to increased survivability through redundancy. In contrast, such weaknesses should be all the

greater in adversary systems. As of March 2002, there are estimated to be 561 million Internet users worldwide. This number is estimated to grow to one billion by 2005 with an online commerce that exceeds $6.8 trillion. This huge amount comprises the projection for both business-to-business and business-to-consumer transactions online. Forrester Research further projects that while the U.S. and North America currently hold the majority lead for online transactions, the lead for online commerce will shift in the coming years as Asian and European nations become more active.[47]

Infosphere dominance, controlling the world of information exchange, may be as complex and elusive as "escalation dominance" appeared to be in nuclear strategy.[48] It will certainly be expensive as the U.S. business community and U.S. armed forces are required to devote more resources and attention to computer, communications, and database security. The resources and skills required for battlefield information warfare are not insignificant, but the resources and skills required to wage information war at the national strategic level would be massive.

The second reason to doubt U.S. ability to prosecute an information war is that the political and legal issues surrounding information war are perplexing. What about Congressional oversight? Would one "declare" information war in response, say, to an Iranian-originated computer virus assault on the FBI's central terrorist database? Then what about the preparations for it? How should the U.S. develop and implement a national capability for information warfare? When does an information attack on the Internet constitute an act of war? Do such declared acts justify a proportional response or an all out physical attack?

While theoretically a requirement to develop or implement a national information war strategy, analogous to U.S. nuclear-era single integrated operations plan, should be

communicated from the President to the Executive Branch agencies, it is unclear whether there would be adequate Congressional oversight. Which committees of the House or Senate would have control and oversight of attendant policies to information warfare? Which would have the power to inquire into the judgment of a local ambassador or military commander who wished to use the tools of information warfare for a perception manipulation in peacetime that would shape the potential wartime environment?[49]

A Demonstrated Capability

Long considered to be the product of capability and will, deterrence was a subject to which much lip service is given but insufficient thought had been devoted. The reason is that general deterrence was usually relied upon to keep the peace. The capacity of the U.S. to conduct information warfare, then, is very great. Its vulnerability to the information warfare activities of others is also considerable because U.S. defenses and will to act are, or perceived as, weak. Deterrence by threat of punishment then centers on the question of will. For deterrence by denial, it is a question of adequate defenses and of how to demonstrate sufficient will to effect focused deterrence. To resolve these issues one has to deal first with the capability to deny, which is centrally a question of strengthening information warfare defenses. Next, the will to punish aggressors, needs to be underwritten by policy statements and other actions that support both general and focused deterrence.

Of the two issues of central interest to the U.S. military, the second, the employment of information warfare, is closely related to deterrence. Employment may be direct or indirect, but it reinforces both capability and will. Its objective is either to discourage information warfare attacks against the U.S. or its friends and allies or to achieve security objectives by offensive action. The use or threat of force occupies a central position in deterrence, but deterrence does

not rely solely on it. For deterrence to be effective, it suffices that an adversary believes that he will be worse off, perhaps more so, for undertaking a particular action than for not attempting it.

Importantly, information warfare tends to be judged by the guidelines governing the use of force: necessity, discrimination, proportionality, and humanity. Clearly, some information warfare actions do not by any stretch of language involve the use of force such as psychological operations, many applications of deception, and also a variety of computer "code bombs," viruses, and "chipping."[50] More importantly, information warfare can be conducted by other than military forces. Such warfare can be waged by a lone hacker, an international terrorist group, a nation state, a rogue corporation, drug cartel, and so on. Thus, what deters a hacker may not deter an international terrorist group or a nation state.

That distinction is an important one, not least because to the extent that information warfare is considered in the same framework as force, its use will be conditioned by four categories of factors: operational, organizational, legal, and moral. Adversaries, or potential adversaries, recognize these constraints and how they affect the will of the U.S. to act or to defend against hostile actions. The overall effect of these constraints on deterrence is not entirely clear, but certainly it is not to strengthen deterrence.

New Arsenals

Given the preoccupation of advanced political economies with the movement of data from point-to-point, it is no surprise that most thoughts about information warfare revolves around DOS attacks shutting computers and networks down. There are a number of problems associated with physical attack that do not apply to information warfare attack. Such thought is unsubtle, inelegant; it shows a lack of understanding of the principles of warfare. It looks more

like a scorched earth policy than any grand strategy and it misses the forest by looking only at the trees. There are many weapons in the information warfare arsenal (see Annex A).

In physical attack, the most catastrophic attack that can be made is directed at the very bottom of the value chain, an aggregate infrastructure of processes, that is where one lives and breathes.[51] This is why there is a perfectly rational fear of nuclear, biological, and chemical weapons. Information warfare is completely reversed, the farther into the value chain any attacks are made, the more leveraged they are and the less force required, just as with the differences between attrition and maneuver-style warfare. Clearly, a more detailed explanation of the relationship between the informational value chain and information warfare is warranted.

The existence of an informational value chain is, in many ways, the defining characteristic of any advanced civilization. For certain adversaries, this very existence is the first element available in information warfare, just as steel won out over iron, having satellites beats not having them, and electronic communication beats an afoot messenger, so to speak. For others adversaries, asymmetric, the use of couriers and courier pigeons may be more valuable in less developed countries. The next step in the chain is intelligence, in the espionage sense of the term. Intelligence is largely a function of the collection of overwhelming amounts of data, and then filtering them down to a usable form. As far back as the dawn of Man, intelligence has been a function that is inherent in information warfare, which comes as no surprise to anyone, least of all people such as Sun Tzu.

Knowing one's place in the value chain helps to explain many of the dilemmas of the intelligence community. Problematic within intelligence is the escalating need and dependence on electronic collection of data countered with the information overload disaster. It is becoming more difficult to keep pace with the increasing load of dynamic data. The problem of electronic

intelligence (ELINT) is that one fails to see the subtleties of motive, intent, and other nuance that human intelligence (HUMINT) used to provide. The inherent flaw of the intelligence process is to remain unbiased. The transformation of data into information automatically calls in to play a archetype, interpretation, judgment, prioritization; this bias is amplified and exaggerated in the process of augmentation.

Information warfare attacks on the civilian value chain infrastructure can actually look more like physical attacks. DOS attacks can range across the value chain, affecting the contributory infrastructure and social contract the way terrorism does. There are common elements of a databased society that attacks will target such as the electronic transport layer thought of as communications, and the control mechanisms are generally relied on as one's "societal glue." An important note is that DOS attacks on civilian entities cannot go farther up the value chain because there is no chain there to target. Military DOS attacks are focused on many of the same elements of command-and-control. This leads to the conclusion that civilian attacks are likely only to be collateral consequences from military objectives. The fear that such attacks will occur are well justified, after all, as the techniques used by guerrillas and terrorists worldwide already map into this new domain.

Whether such attacks work is another thing altogether, much of the low end of the military informational value chain is already hardened, notably a by-product of the nuclear age. Satellites have always been assumed to be expendable, and military command-and-control has been a target in millennia of warfare. The capture of a commander in a hierarchical structure is more effective than trying to grind down troops. This sort of information warfare attack is survivable, correctable, and will cost a great deal in damages. However, much like Pearl Harbor in World War II, it is likely to only infuriate the population of the targeted political economy.

More subtle methods of DOS attacks may be effective. Historically, when analysis and decision-making power were seated in the same person, these were worthwhile targets. In modern times most politicians are perpendicular to the informational value chain, providing no added value. The tools in place to provide such added value are, however, directly susceptible to such attack, and in many cases are not even protected.

Assume for example, that an adversary planned a conflict and wanted to impair the decision-making abilities of a powerful, advanced ally of their target. Are attacks on orbiting satellites that provide data on their region even possible, let alone cost effective? Not likely, but an adversary can bring other resources to bear on that problem. Imagine this chain of events:

(1) A set of video cameras is placed so that they collect data, the license plates of vehicles going into the "hostile" intelligence agency.
(2) Data is continually collected and processed.
(3) The license plates are checked for in a variety of databases to provide the name and any other data on the owner and likely driver.
(4) The driver's credit and personal data is pulled, as well as any other information that can be checked from the ever-growing number of databases.
(5) Based on the data derived, a structural map of the organization is developed, founded on such things as salary levels, education level, specialty, etc.
(6) Certain functions are targeted, such as analysis sections or skill bases, such as knowledge of an adversary's region or language.
(7) Just prior to hostilities, such individuals are targeted for either subversion or elimination.

This sort of DOS attack is directly targeted at the deeper levels on the informational value chain, those with knowledge or wisdom about the region and adversary. It has many benefits besides being cheap, direct, and leveraged. It leaves the political players "in the game," but without any method to make sense of the overwhelming levels of data, or information overload, prior to or during a conflict. Because of the common mechanism of reliance by the military on politicians to set objectives, any coherent military response by the targeted country is also hamstrung. It doesn't require great skill to carry out this sort of attack. But the impact,

particularly the transformation of the political structure into one of value subtracted, is considerable. Recovery from such an attack is a matter of luck in making all the right choices in the time period it takes to rebuild the lost functionality, an unknown period, but far longer than rebooting a computer and reinstalling software as after a DOS attack.

A true information warfare attack is one that covertly distorts information. In the terms of an old military adage, war is deception. People make decisions based on their cognitive environment, their infosphere. The control of the data comprising such an environment allows a certain amount of control over those in it. The drawback is that the better the information of the adversary about their infosphere, the closer the deception must be to the reality provided by the environment. Very much a situation of Garbage In, Garbage Out (GIGO), this sort of attack is about the use of lies and mis/disinformation to produce very real results. It can be very direct, and successful, when say surrendering when you only think you are surrounded but are not. It is the use of inflatable tanks and airplane skeletons to misdirect thinking regarding the time and place of an attack. Such attacks will become more prevalent and subtle when direct control of data channels is possible. The double-edged sword of the media can be grasped more directly than was CNN by the West during the Gulf War, and to much better effect, but care must be taken to avoid the sapping of will that occurred during the Vietnam conflict.

OODA loop or OODA point

Information warfare is ideally suited for the command, control, and execution of military operations across the spectrum of warfare from the selective release of non-lethal weapons to the full-scale assault of parallel war. In parallel war, military forces simultaneously attack adversary centers of gravity across all levels of war (strategic, operational, and tactical) at rates faster than the adversary can react.[52] Commanders always seek to control the throttle of the observe, orient,

decide and act (OODA) loop, operating faster while slowing the decision cycle of one's foe. For example, in Figure 3 one can see that OODA loop B is larger than A, which means that it takes longer for B to make a decision. The objective is to increase your adversary's OODA loop while speeding up (shrinking) your decision loops. Looking at the graph in the middle, as the OODA loop shrinks it theoretically can reach a loop that is virtually a point. With the advent of information technology, processor speeds are increasing at almost logarithmic proportions every few months. This means that data can be processed faster and hence speed up one's OODA loop, approaching an OODA point.[53] In similar method, information warfare weapons allow one to expand the adversary's OODA loop through denial, disruption, destruction, or mis/disinformation increasing the adversary's decision-making time.

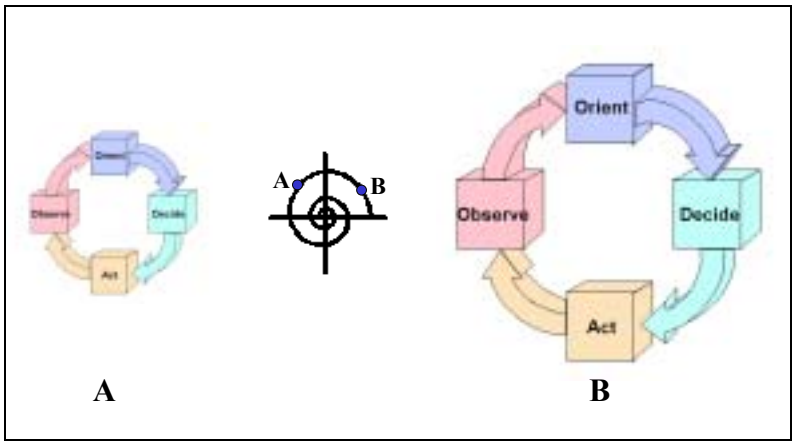

Figure 3. OODA Loop

In past wars, tank commanders and fighter pilots always strove to get inside the adversaries' OODA loop. The difference in future conflicts will be the speed and scope of their decisions. Parallel war requires large numbers of highly precise weapons directed against critical nodes. Additionally, they require a requisite level of detail on the adversary situation necessary for precision targeting. For these reasons yesterday's military commanders could not wage parallel war effectively.

Information warfare is ideal for conducting parallel war because it offers capabilities that fills both of these voids. It offers commanders a near real-time view of the battlespace, exposing the adversary centers of gravity before his eyes. Operating at previously unheard of speeds will be a common feature of military engagement. Future wars will utilize a whole new array of air and space sensors, UCAV, directed energy weapons, and highly mobile expeditionary forces. Operations will be controlled from the continental U.S. (CONUS) and instantaneously reach out and touch the adversary halfway around the globe as demonstrated recently by B-2 stealth bombers.

A CONUS-based joint task force commander, for example, would have well exercised connectivity with combat units through integration with CONUS-based B-2 stealth bombers, UCAV, and instantaneous access to space based precision strike weapons. Imagine the psychological effect on the adversary who will be unable to predict where the next blow will fall and will be powerless to defend against it.

U.S. force structure and battlespace requirements will make obsolete traditional hierarchical command-and-control arrangements. Information warfare capabilities require greater decentralization through information technology, growth of distributed systems and establishment of virtual organizations. In fact, "new information and communications technologies are shifting power to those with the most powerful computers and most effective sensors . . . at the same time, the punch packed by the individual soldier is increasing, eroding the role of field commanders and resulting in flatter command-and-control structures."[54]

In information warfare there will be greater emphasis placed on decisive decision-making, precision engagement, high-speed and synchronized maneuver, agility, and enhanced command-and-control. The command structure will need freedom of operation within

previously identified parameters much like German *Auftragstaktik* (mission tactics), a decentralized, flexible command style. This method of battlefield command enables smaller forces to defeat much larger ones through a timely ability to seize the initiative and act according to "on the spot" judgment. The German breakout at Sedan, resulting in the fall of France in 1940 offers a familiar example of the successful employment of this flexible command philosophy.[55]

The warfighter must have access to a broad range of supporting weapons, improved mobility, survivability, and supportability. Changes should reflect a dramatically flattened command structure staffed by an extremely high caliber individual at every level. As the battlefield becomes less dense and more decentralized, the demands on small unit leaders increase. A flattened structure permits power to be defused and redistributed, often to subordinate actors. The overall impact is that the flow of information, and its associated awareness and knowledge, compels closed systems to open, eliminating many layers of the cumbersome and compartmented intelligence and analysis bureaucracy. The traditional emphasis on command-and-control will give way to an emphasis on consultation and control.[56] Such an organizational structure permits the commander to operate at maximum efficiency. It allows operations at all levels with greater latitude and autonomy as part of an integrated joint operation, a truly combined arms effort. Information warfare tools will provide enormously enhanced capabilities and opportunities for the warfighter. These tools do alter some the fundamental principles of war such as objective, mass, economy of force, maneuver, surprise, and simplicity. But these principles guide warfighting at all levels of warfare and having withstood the test of time, will endure as the bedrock of U.S. military doctrine.[57] Information warfare optimizes the principles of offense, mass, and maneuver, enabling the commander to

execute a wide array of precision weapons from CONUS across the spectrum of warfare at a single decisive point or a parallel attack against multiple critical nodes.

Vulnerabilities and Shared Threats

As seen from the opening example, the U.S. is vulnerable to shared threats that not everyone can agree upon. A key problem for those focused on protection is that they have suggested, but cannot yet demonstrate, the real consequences as opposed to theoretical susceptibility or vulnerability to serious disruptions. This is different from recognizing the serious potential consequences to modern societies if destruction of critical systems should occur. As a result, it will be difficult to employ strategic information warfare as a deterrent until such time as the effects of the opening example are demonstrated.

The U.S. Air Force has recognized the difficulty of identifying specific information targets and has attempted to address the issue through its *Cornerstones of Information Warfare* pamphlet and new doctrinal documents. For example, the Air Force has stated "information warfare is any attack against an information function, regardless of the means."[58] Therefore, bombing a telephone switching facility is considered information warfare. So is destroying the switching facility's software.[59] Similar types of targets may then include elements of the adversary integrated air defense system (IADS). In defining the information target, the U.S. Air Force has attempted to focus information warfare as "a means, not an end, in precisely the same manner that air warfare is a means, not an end."[60] However, an unintended consequence may result from this overarching target definition: if information warfare encompasses nearly every target, then the concept merely becomes a new label for traditional military operations (e.g. psychological operations, deception, physical destruction.) that military forces have conducted for thousands of years.

Others cite the effects of an information attack against the information target as capable of "wield[ing] the power to blind, deafen, muzzle and mislead their adversary by poisoning or crippling their computer systems."[61] This is reminiscent of the type targets that Colonel Tanksley relayed in his information warfare Armageddon scenarios whereby computer viruses and logic bombs bring down an entire nation.[62] Do information weapon attacks against communications and control facilities, the adversary's IADS, and their computers diminish adversary will and capacity to fight? Does information warfare reduce the OODA loop to such speeds as to now call it the OODA point? Well, yes and no. Certainly, "hard killing" elements of the adversary information functions or "soft killing" through introduction of viruses and logic bombs into the adversary's computer systems would affect his capacity to fight. Hard kills result in the physical destruction of information systems and interconnectivities, while soft kills render computer screens "blank" or cause the systems to present faulty displays.

Given that the information weapon could affect an adversary's capability to fight, will it also be able to affect his will to carry on the fight? While the adversary computer terminal operator may feel disheartened and experience decreased morale resulting from leaders' demands for unavailable information, the latter's will to fight may or may not be affected. In other words, how would "blinding" adversary leaders affect their will to fight? Would they actually surrender or would U.S. "blinding" operations actually backfire and force adversary leaders to panic and resort to the use of weapons of mass destruction? For example, Russia adopted a military doctrine in November 1993 that indicated a belief that during a East-West conflict, an attack on Russia's early-warning system for strategic nuclear forces was possible.[63] In such a situation, the Russians assumed the worst, the invasion of Russian territory by foreign military forces. With their sensors blinded and command-and-control systems destroyed by

information weapons, Russian leaders would not be able to obtain information and would resort to whatever means necessary to protect their homeland. In essence, they would be "blind" but their strategic nuclear weapons would still be intact and operable. How can the information warfare advocate be certain that Russia would not employ the nuclear weapons?

Instead of just dwelling on whether information warfare attacks will affect an adversary's will to fight, one should ask how U.S. military leaders would react if an adversary blinded friendly command-and-control systems? Would U.S. military leaders lose the will to fight if their computers went blank? The will to fight is an elusive target and it is difficult to assess whether the information warfare attack is capable of affecting it. Certainly, other factors such as political objectives and whether the adversary is fighting for its own survival or for more limited goals would surely figure into the "will to fight" equation.

Perhaps those who advocate using the information warfare against the second type of information target, the "adversary mind's ability to observe and orient" place more importance on the morale factor than the physical. Champions of attacking this type of information target have coined this form of information warfare as "perception management,"[64] Perception management is "manipulating information that is key to perceptions" and has also been labeled as "orientation management," or "neocortical warfare.[65] While these terms may imply some "new" types of warfare, in actuality, they are merely loose terms for what had been traditionally called psychological operations, propaganda, and military deception. For the purpose of discussion, this form of information weapon will be considered perception management.

The same question posed about information as a target also applies to the adversary mind. The key question is whether information warfare will necessarily reduce the mental ability and will to resist. While perception management can deceive, surprise, add to the adversary's fog

and friction, and affect the morale or the will to fight, it will not likely produce a "predictable error" as assumed by Dr. George Stein.[66] The concept of producing a "predictable error" implies that one can predictably stimulate advantageous errors in the adversary's actions and OODA loop. Basically, it assumes that human behavior and reactions are totally predictable and may be accurately manipulated with some degree of precision. This goes against Clausewitz's philosophy of the unpredictability in humans and warfare.

Not only does the concept of "predictable error" ignore Clausewitz's theory regarding human nature and warfare, it also challenges reasoning. Is it really possible to predict the actions, intent, and decision-making rationale of such disparate minds as those of Adolf Hitler, Josef Stalin, Ho Chi Minh, Ayatollah Khomeini, Muammar al-Qaddafi, Saddam Husayn, Mohammed Aideed, Kim Chong-il, or Usama Bin Laden? Hitler thought he could achieve his predicted outcome when he drew up his "Barbarossa" plan and "believed nothing less than the Soviet Union could be defeated in four months."[67] But by April 1945, Soviet tanks entered and captured Berlin, fours years after German forces invaded the Soviet Union. A "predictable error" is usually very difficult to predict, much less to produce.

In the same vein, perception management will likely have minimal impact on the adversary's capacity to fight, unless, of course the information attack deceives the adversary regarding the disposition and location of friendly forces. As an illustration, the World War II Allied deception plan, Operation Fortitude, contributed to Hitler's preconceptions of the location of the impending invasion of France would be at the Pas de Calais. Consequently, invading Allied forces at Normandy did not face the bulk of the German troops in France and Belgium guarding the Pas de Calais and the Belgian and Dutch coastlines.[68]

In the ideal world, fog and friction should be eliminated for friendly forces while being maximized against the adversary. However, the exact information weapons intended to increase the adversary's "fog of uncertainty" may lead to totally unintended consequences inconsistent with the original intent of the weapon. Worse, 2nd and 3rd order effects may actually prove counterproductive to the original intent and objective. In a complex, hierarchical command-and-control system, destruction of selected communications connectivity may actually result in a more streamlined and efficient command-and-control system.

Unintended consequences could allow an adversary leader, without the intermediate command-and-control steps, to send his orders directly to the lower echelons. For example, during Desert Storm, after coalition forces destroyed Saddam Husayn's more advanced telecommunications capacity, he continued to send launch orders to Scud missile batteries via courier.[69] If adversary communications connectivity is cut off, lower echelons will likely operate in autonomous modes. While they may lack the complete situational battlefield picture that upper echelons would normally provide, the lower echelons benefit by not having to wait for launch orders to flow from the top. Finally, destroying or degrading adversary command-and-control systems may deny friendly forces the ability to collect critical adversary communications and signals. Thus, employment of an information weapon may actually abridge adversary operations and increase friendly fog and friction, since friendly collection assets will not be able to collect against emitting adversary electronic systems.

Perhaps the most troubling claim is that of an information weapon's capability to attain quick and bloodless victories and the extreme view of preventing a war before it starts. While information warfare may be able to prevent bloodshed in some scenarios, expecting it to end a war before the first shot is fired is pure conjecture. A more realistic consequence resulting from

the employment of an information weapon would be a degraded adversary that lacks complete battlefield situational awareness because leaders are blinded and cannot communicate with troops in the field. There is no historical evidence that supports the concept that a blinded adversary would simply surrender without fighting. Quite the contrary, history shows military forces, isolated from its headquarters, do continue to fight. As previously mentioned, the German military, during World War II, emphasized *Auftragstaktik*, which relied on general guidance from above combined with lower echelon initiative.[70] This philosophy resulted in German forces fighting under radio silence, without upper echelon guidance, as happened during the Allied Normandy campaign.

Major General Michael V. Hayden, former commander of the Air Intelligence Agency, summed it best when he called the "notion of a bloodless war played out on computers as fanciful" and said that he does not foresee the U.S. mothballing its stockpile of conventional and nuclear weapons in the near future. Further, he stated, "Can I imagine a time in which we won't have destructive war? No. But I think it's easy to imagine a time when we can use information as an alternative to traditional warfare." General Hayden relayed the following incident to describe the use of the information weapon to help create the zone of separation between warring factions in Bosnia:

> Some of the factions didn't comply completely. But the Implementation Force goaded, forced, cajoled and pressured them to do it. One of the things they did was take clear evidence [and] information that they had not complied with the treaty. The IFOR commander turned to the Serb, the Croat and the Muslim and said, "Move those tanks." Their response was "What tanks?" The commander says, "These tanks," pointing to the concrete evidence. "Oh, those tanks," they said. And then the tanks were moved. In Bosnia, I think it's fair to say, information is the weapon of first resort. To back that up is the potential for heat, blast and fragmentation. But in this case, information was used as an alternative. We achieved an objective without going immediately to some sort of destructive approach.[71]

It is clear that while information can be used as a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to blind the adversary prior to conventional attacks and operations. The U.S. military arsenal includes a variety of weapons and the strategist must ensure their most effective use in future wars. The strategy of the future will likely include the use of the information weapon in conjunction with more conventional weapons. In developing the campaign plan, the strategist must realize that the use of information weapons will demand caution and carry implications that may impact the use of these weapons.

Vulnerability to an adversary using information warfare weapons and tools was examined during a military exercise conducted in early summer of 1997. The scenario featured "scripted" attacks on the energy and telecommunications infrastructures. The controllers injected incidents into the scenario where military commands and government agencies reacted as though the reported incidents were real. Companies providing electrical power in selected cities were subjected to scripted attack by cyber means, over time, in a way that made the resulting simulated outages appear to be random and unrelated. Concurrently, a "Red Team" used hacker techniques available on the Internet to attempt to penetrate DoD computers. With no insider information, and constrained by U.S. law, the team spent three months probing the vulnerabilities of several hundred unclassified computer networks. They were able to penetrate many of these networks, and even gained system administrator level privileges in some.[72]

Simulated information warfare attacks on nearby privately owned energy companies and telecommunications service providers and successful penetrations into DoD computers were assessed by controllers as sufficient to have disrupted operations at selected military bases. This

created the situation in which the U.S. ability to deploy and sustain military forces was degraded. Was this exercise an over-statement of today's vulnerabilities or a glimpse at future forms of terrorism and war? The experience to date, the known vulnerabilities, and the continuing pace of change suggest the latter. The day may be coming when an adversary can attack the U.S. from a distance, using cyber tools, without first confronting U.S. military power and with a good chance of going undetected. The new geography is a borderless infosphere whose major topographical features are technology and change. A good offense may prove to be a better defense.

To defend against the threat one should concentrate on understanding the tools required to attack computer systems in order to shut them down or to gain access to steal, destroy, corrupt or manipulate computer data and code. In addition to accidents and negligence, threats to computer systems cover a broad spectrum that ranges from prankish hacking at the low end to organized, synchronized attacks at the high end. But the basic attack tools, computer, modem, telephone, and user-friendly hacker software, are common across the spectrum and widely available.

Potential information warfare threats and associated risks range from recreational hackers to terrorists to national teams of information warfare specialists. Repeatedly identified as the most worrisome threat is the insider, someone legitimately authorized access to a system or network. One's adversaries may make use of insiders, such as organized crime or a terrorist groups suborning a willing insider (e.g. a disgruntled employee) or making use of an unwitting insider by getting someone authorized network access to insert a disk containing hidden code. Five examples of new types of attack may help illustrate the way commonplace information warfare tools can be used to do harm:

(1) An information warfare attack on the specific databases of an owner/operator allowing unauthorized entry into a network or system for the purpose of illegal

financial transfers, stealing proprietary information, disrupting records, or merely browsing.

(2) An information warfare attack for the purpose of gaining network access. A particular system or network is discovered through "electronic reconnaissance" with low security standards and is interconnected to other networks of interest to the attacker, which becomes a pathway for access to the targeted system.

(3) An information warfare attack for the purpose of espionage by a witting or unwitting insider, unscrupulous competitor, or the intelligence service of a foreign power. Competitive advantage may be lost without knowing it was even at risk whether it is business or government system.

(4) An information attack for the purpose of shutting down service—DOS attack. This attack floods communication lines to shut down e-mail service to major users, which are of concern to all institutions whose business depends on reliable communications.

(5) An information warfare attack for the purpose of introducing harmful instructions by planting a virus or leaving behind a program that will give the attacker critical information, such as passwords that can be used to log in to other networks. Viruses are transmitted within a local area network or passed on to an external net while "Logic Bombs" and "Trojan Horses" are designed, respectively, to destroy software at a pre-selected time to enable future access.

These new types of attack are not from the typical State actor but non-State actor and are difficult to detect and identify the actual perpetrator. Indeed, such information warfare attacks are increasing in complexity, ingenuity, and frequency.

The technologies of information warfare offer opportunities to consider old concepts in new ways. For example, trade and economic embargoes have been traditional tools of coercion and deterrence. Embargoes have concentrated on stopping the flow of goods and materials from entering a country. The success of such an embargo was largely based on the dependence of the country on the embargoed goods and materials as well as one's ability to execute the blockade. The more dependent a country is, the greater chance for success. This same concept applies to information warfare as modern societies are based on the access to information. Thus, the ability to stop the flow of information into another country can be an effective embargo-like tool in imposing one's will upon that country. Not unlike past embargoes, an information embargo could totally isolate a country from essential electronic information of all sorts from all sources

or it terminates information that provided to that country. The success of an information embargo is based upon the dependence of that country on the information being blockaded. However, unlike embargoes of goods and materials, information blockades become less feasible as borders are not barriers to information.

Simply then, the U.S. concept of deterrence, whether criminal or military, is based on building a credible belief in the mind of a potential adversary that the attack will be met by an unavoidable and unacceptable counterattack, or simply the U.S. will go on the offense. The nature of such a counterattack, in order to maintain credibility, depends in part who the attacker is, on the nature of the attack, and on the attacker's vulnerability to counterattack.

The military and civilian communities share such common vulnerabilities to an attack that suggests that a common understanding of the threat and a common approach can provide an effective defense as discussed in the next section. Understanding the deterrent capabilities of information warfare and the anxiety about using it offensively sheds light on its constraints. How does the U.S. effectively organize for information warfare? What are the command-and-control issues surrounding its use? Would there be different structures for defensive and offensive information warfare? How would these be organized? The next chapter will examine how the U.S. is organized, or not, for information warfare and how effective is it?

Notes

[37] Waller.
[38] Howard Frank, director of the Information Technology Office of the Defense Advanced Research Project Agency, quoted in Steve Lohr, *Ready, Aim, Zap*, New York Times, 30 September 1996, pg. D-1.
[39] U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD 96-84, General Accounting Office, Washington, DC, May 1996; and Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare--Defense (IW-D)*, Office of the Secretary of Defense, Washington, DC, November 1996.
[40] The Commission was formed by Executive Order 13010, 15 July 1996. The "critical domestic infrastructures" identified in the executive order are: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.
[41] Chairman, U.S. Joint Chiefs of Staff, *Command-and-control Warfare*, CJCS Memorandum of Policy (MOP) 30, The Joint Staff, Washington, DC, 8 March 1993.

Notes

[42] Libicki, Martin C., *What Is Information Warfare?,* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, Washington, D.C., August 1995.
[43] U.S. Department of Defense definitions of information operations: " Actions taken to affect adversary information and information systems while defending one's own information and information systems," and of information warfare: " Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."
[44] Wallich, Paul, *A Rogue's Routing*, Scientific American, 272, no. 5, (May 1995), pg. 31.
[45] Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway,* Thunders Mountain Press, New York, NY, 1994.
[46] Pichot-Duclos, Jean, *Toward a French `Economic Intelligence' Model*, Defense Nationale, Jan 1994, pp. 73–85, in Federal Broadcast Information Service - West Europe, 25 January 1994, pp. 26–31.
[47] *Global Internet Statistics (by Language),* retrieved 25 March 2002 from the World Wide Web, http://www.euromktg.com/globstats/index.html.
[48] Joint Chiefs of Staff Memorandum of Policy 30, *Command-and-control Warfare,* 8 March 1993.
[49] Griffith, Samuel, *Sun Tzu, The Art of War*, Oxford University Press, New York, NY, 1971, pg. 110.
[50] Magsig, Daniel E., *Information Warfare in the Information Age*; George Washington University, 7 December 1995. "Chipping" is the practice of making electronics chips vulnerable to destruction by designing in weaknesses. For example, certain chips may be manufactured to fail upon receiving a specific signal.
[51] A value chain is an aggregate infrastructure of processes. An example comes from Man's early days and metal. Based on what ores were readily available in an area, Man built a variety of implements, starting with rough-hewn rock or wood, moving via the process of discovery and learning to more complex substances--iron, bronze, and steel. Years and centuries pass, and the materials, knowledge, and processes that started turning out plowshares now turn out automobiles, airplanes, bridges, and skyscrapers. Each step in the process, each advance made, adds just a little more value to the output of the previous step, building vastly more complex systems from the interactions of numerous smaller ones. Politics is about the ownership and control of the value chain. Western democracies are based on principles that every individual owns themselves and the fruits of their labor, that they are each entitled to an equal opportunity to be responsible for themselves. Western governments are the tools, the value chain the citizens created to gain an economy of scale--to do those things collectively that are best done so. Among such things is the provision of a common defense, in short, war. War, then, is a challenge to or fro m the value chain. Just as the discovery of steel heralded a new wave of conquests against those less developed, war is the competition of value chains. Whether fought with steel swords, or composite-armor tanks, conventional and unconventional warfare are about attacks on various stages of the material value chain, by methods best suited to the attack on each link. War, then, is an obsessive emphasis on the real control of real things, in methods, means, and end objectives.
[52] Barnett, Jeffrey R., Future War: *An Assessment of Aerospace Campaigns in 2010,* Air University Press, Maxwell AFB, AL, 1996, pg. 6.
[53] Kaspar, Beth M., Air University, *The End Of Secrecy? Military Competitiveness In The Age Of Transparency*, Maxwell Air Force Base, AL, April 2000, pg.64. Also Hammonds, Grant T., *The Mind of War: John Boyd and American Security*, Smithsonian Press, Washington, DC, 2001, pp. 118-174.
[54] Institute for National Strategic Studies, *Strategic Assessment 1995: US Security Challenges in Transition,* National Defense University Press, Washington, DC, November 1994, pg. 16.
[55] Doughty Robert A., *The Breaking Point: Sedan and the Fall of France, 1940,* Archon Books, Hamden, CN, 1990, pg. 3.
[56] Kasper (Also Hammonds).
[57] Joint Warfghting Center Doctrine Division, *Warfighting Vision 2010: A Framework For Change,* Langley AFB, VA, 1 August 1995, pg. 2.
[58] USAF, *Cornerstones of Information Warfar*e, 1995, pg.4. Therefore, "bombing a telephone switching facility is information warfare. So is destroying the switching facility's software."
[59] *Cornerstones*
[60] *Cornerstones*
[61] McKenna, Pat, "*Info Warriors: Battling for Data Dominance in the Fifth Dimension*," Airman Magazine, September 1996.
[62] Waller.

Notes

[63] Boll, Michael M. and Holcomb, James F., *Russia's New Doctrine: Two Views*, Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA, July 20, 1994.
[64] George J. Stein, *Information Attack: Information Warfare in 2025*, in 2025 White Papers, vol. 3, Book 1, ed. 2025 Support Office, Air University Press, Maxwell AFB, AL, November 1996, pp. 91-114.
[65] Szfranski, Richard, *Neocortical Warfare? The Acme of Skill*, Military Review, November 1994, pg. 45.
[66] Stein, pg. 114.
[67] Overy, Richard, *Why the Allies Won,* W. W. Norton & Co, New York, NY, 1995, pg. 13.
[68] Overy, pg. 151.
[69] Gordon, Michael R. and Gen Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf*, Little, Brown and Co, Boston, MA, 1995, pp. 246–48; and Steven K. Black, *Information Warfare in the Post–Cold War World*, University of Pittsburgh, 1996, pp. 246-248.
[70] Depuy, Trevor N., *A Genius for War,* Hero Books, Fairfax, VA, 1984, pg. 4. Also DiNardo, R. L. and Daniel J. Hughes, *Some Cautionary Thoughts on Information Warfare*, Airpower Journal 9, no. 4, Winter 1995, pg. 4.
[71] McKenna, *Info Warriors: Battling for Data Dominance in the Fifth Dimension*, Airman Magazine, September 1996.
[72] ELIGIBLE RECEIVER, in June 1997, was the first large-scale exercise designed to test our ability to respond to an attack on our information infrastructure. Designed to test DoD planning and crisis-action capabilities, it also evaluated our ability to work with other branches of government to respond to an attack on our National Infrastructures. ELIGIBLE RECEIVER revealed significant vulnerabilities in our information systems and the interdependence of the defense and national information infrastructures. It showed that we had little capability to detect or assess information warfare attacks and that our "indications and warning" process for cyber events was totally inadequate.

Chapter 5

Organization

The use of force by the U.S. is constrained by the way the country is organized. Democracies are historically more reluctant to use force than are other types of government.[73] For example, the Commander-in-Chief is the President but the power to declare and support war lies with the Congress. Thus Congress is a source of constraint on the use of force. If information warfare is regarded as the use of force, especially if those operations are preemptive or a first use, then consideration must be given to how to deal with these problems. Similarly, many forms of freedom and rights to privacy, including personal information, are considered to be fundamental in the U.S. These have great import for the conduct of information operations, in particular when attempting to track or trace the source of attacks on the nation's infrastructure. Strong legal and societal forces are highly resistant to governmental monitoring of, or interference in, the unfettered flow of information, plain or encrypted although such resistance tends to abate in times of war.

The Mission

The information warfare battlefield mission would seem obviously to be a role of the DoD as would any strategic offensive role. But strategic defensive responsibilities are not as clear due to other organizational hindrances such as the freedom of the press, which in the U.S. represents another source of restrictions. The power of the media to raise difficult questions and issues should be considered before information warfare is undertaken. Then there are the constraints posed by external organizations of which the U.S. is a member, most notably the

United Nations and NATO. Mere membership in these organizations means acceptance of additional layers of constraint and ad hoc coalitions have a similar restrictive effect.

That begs the question, on organizational issues, who does what in this arena? The general answer should be that, to be fully effective, appropriate offensive information warfare "weapons," for example, should be added to the repertoires of all elements of forces. These are weapons, as an application of force, can be used across the whole spectrum of war. That spectrum ranges from psychological operations to tactical deception to the whole range of ground-attack operations. Not only would such integration make using the weapons effectively much more desirable, but also it would help place "information warfare" techniques and technologies in a more useful operational context. Similarly, defensive information warfare needs to be instilled into all organizations responsible for acquiring and/or operating information systems. Better exploitation of information is everyone's business. However, the focus of this monograph is on the military role, not civilian organizations. Integrating information-related concerns into the whole spectrum of military operations would help guide decisions about the relative weight to give information warfare, as opposed to more traditional approaches. This could provide the basis for the military to evolve into a completely different kind of organization with a different culture and real emphasis. In the meantime, the Services need to establish information-related career paths within their existing structure and avoid creating a "computer geek command" that would isolate rather than integrate personnel with expertise on information technology and applications.

This sort of organizational approach should also produce a more specialized, differentiated set of skills and responsibilities rather than lumping quite unrelated career field specialties together into an umbrella information warfare organization. This should help resolve

the inevitable roles and missions conflicts that will arise among competing Services and Agencies. That is particularly important in the relatively short term when critical information-related skills are likely to be in too short supply to permit much duplication in functions among organizations. Some critical skills are more likely to exist in such organizations as the National Security Agency, the Central Intelligence Agency, and the Defense Intelligence Agency than in the uniformed services. Sorting all this out should be part of the national-level debate on roles and missions of the military, the intelligence community, and the rest of the DoD.

So far, the Air Force has rejected the concept of an information warfare command or its equivalent. Establishing such a command would delay rather than promote the necessary integration of information-related considerations into the whole spectrum of Air Force operations. Also, the Air Force has given the Air Staff (Plans and Operations) and Air Combat Command primary responsibility for information warfare issues. However, these organizational issues are far from resolved. The responsibilities and rules of the newly created (or, in some cases, renamed) organizations, such as the Information Warfare Center and the many Information Warfare Squadrons, as well as the more established organizations, such as the Air Force C^4 Agency, remain to be sorted out.[74] Similarly, creating information warfare organizations within established groups could be counterproductive if the net effect is to isolate rather than integrate the responsibility for information warfare-related considerations. At best, the jury is still out on how well these institutional solutions are going to work. Ironically, the existing institutional structure was probably sufficient if only it had been used effectively.

The Roles

The nature of information warfare is not exclusively a military sphere of influence. Assuming an adversary launched a information warfare attack on the U.S., what role should the

military take in response? Should the military take the lead because others view such an attack as both an act of war and a national defense issue? Both information warfare and biological agent attacks cross this difficult line. What makes these attacks different from a nuclear warhead delivered by a missile? The distinction seems to hinge on whether the issue is:

(1) To defend against an information warfare attack.
(2) To deal with the domestic consequences of the attack.

If the military is to lead the effort for information warfare defense, it should be prepared to deal with potential resistance from other federal agencies such as the Federal Emergency Management Agency (FEMA) or the Department of Justice. Others would add the Departments of Commerce, Treasury, Health and Human Services, Energy, Transportation, State, and the Environmental Protection Agency. All could play key roles, depending on the attacked target. If it is domestic (a crime) then the FBI would take the lead, but if it is international in origin (an attack) then the DoD would take the lead. The military should assume the supporting role during information warfare attacks to the homeland until the attack is clearly defined as a threat to U.S. vital interests and the responsibility among federal agencies is delineated.

Moreover, a litmus test is needed to assess whether an information warfare attack even constitutes a direct attack to U.S. vital interests. When does such an attack become a weapon of mass destruction or mass disruption? Should a distinction be made between destruction and disruption to craft an appropriate military response? The issue requires further debate and exploration to produce a practical and workable strategy. Another challenge is identifying the attacker because it could simply be curious teenagers or disgruntled insiders. But, if hostile nations or known terrorists initiated the attack, the U.S. military should likely retaliate.

Conversely, the military lead role outside the homeland is well defined such as the actual role the military played in the information war in Kosovo. Bob Brewin, Federal Computer

Week, reported that a London-based spokesman for U.S. Naval Forces, Europe, confirmed "it was the first time a Joint Task Force staff was organized with an information operations (IO) cell, which was composed of military personnel with expertise in various facets of IO.[75] The IO cell objective was to disrupt Serbia's computer systems to give the U.S. and her allies the winning edge in the information warfare. Dealing with the military side of information warfare begs the more fundamental question of how to protect U.S. society in general from attacks on its information infrastructure. One needs to understand the broader problem in formulating an approach to information warfare by the right questions. How serious is the problem? What can be done, and how well is it likely to work? Who can or who should do it?

The problem has certainly captured the imagination of authors and raises some intriguing questions about the very nature of conflict. It has been noted that it is difficult to tell in the information age if a nation were at war and, if so, with whom. In addition to potentially hostile nations, probable adversaries could include criminals, hackers, terrorists, insurgents, and industrial interests. The particularly attractive feature of this kind of warfare is that while it requires considerable expertise, it probably does not take much in the way of resources or involve much physical risk to the attackers. Thus, it may offer many "wannabes" a set of weapons to use against the perceived U.S. hegemon.

The Threats

The difficulty comes in attempting to define the severity of these threats. Anecdotal evidence on past and present events, while abundant, is not useful in this regard because it is not clear whether these anecdotes represent the tip of the iceberg or an comprehensive list of all incidents. Better evidence is hard to come by, partly because data are simply difficult to obtain and partly because some classes of victims (e.g., banks and other financial institutions) have

every reason to keep such incidents quiet. This considerably complicates both analysis and solving problems related to information vulnerabilities. It also raises complex questions about where the private responsibility of institutions stops and the government's responsibility for protecting the broader public interest start, as well as where in government does (or should) the expertise reside to deal with the problem. Even the legal issues associated with the government's accessing details about private information systems to protect them adequately and with sharing information on computer vulnerability with private organizations are likely to be overwhelming.

It is difficult to know the magnitude of the potential problem without examining the vulnerabilities and failure modes of the countless information systems upon which various parts of U.S. national interests depend. Electronic funds transfer network, the air traffic control system, and the electric power grid control system are only a few of the many pieces of the information infrastructure on which U.S. national interests rest. Each of these is protected to some degree from some set of threats, but not all threats. Locating and adjusting the chinks in one's information systems armor should be a national priority if the U.S. is to take the threat of information warfare seriously. The challenge facing a potential adversary is to find the vulnerabilities and exploit them before they are corrected.

Civil Response

The Computer Security Act of 1987 gave the responsibility for the protection of the National Information Infrastructure (NII), to the National Institute of Standards and Technology and to the National Computer Security Center, which is a part of the NSA. Neither agency has the budget, power, nor expertise to effect real changes in the manner that computer systems vital to the national interest are protected. More importantly, they do not have any legal authority to do so when those systems are owned and operated by private companies, as are the electric

power grid, telephone networks, etc. Nor can they alone referee questions of competing military and civilian interests. NSA involvement is a particularly delicate political and legal issue, given its primary mission as a collector of foreign intelligence and designer of U.S. cryptography systems. NSA probably has the largest concentration of expertise on information security in the U.S. government, thus involving it in some politically and legally acceptable maneuver would be essential unless its technical skills and experience could be reproduced. Otherwise, the task is likely to be left to organizations, such as the FBI, that have appropriate charters but lack the expertise or the organizational culture to do the job effectively. An interagency approach or even a consortium that enlists the skills of industry experts might eventually prove adequate. If they developed ample expertise in the area and were legally permitted to do so, the Services could be a key player, as well as a key member of such an interagency team. That would certainly be a different role for the Services, but one that might be both important and appropriate for the future.

None of this is likely to happen soon, however, until there is a detailed national policy. Such a policy should define the national interest in the information arena, establish a mechanism for setting priorities among information operations objectives, and assign responsibility for enforcement. Establishing this national policy should be a priority item, especially as a part of Homeland Defense measures. The need exists and actions are in work towards formulating such a national strategy on information war.[76]

Military Response

The 21st century U.S. is not accustomed to seeing its military involved in domestic affairs, except during national disasters, emergency, and riot situations. However, there will be increasing roles and missions for the military in homeland defense that go beyond their

traditional role. Nevertheless, examples of the military providing disaster relief are not unprecedented. Recall the military assistance in the Oklahoma City bombing, the World Trade Center bombing, and other disasters.[77] The Constitution clearly defines the role of the military to be subordinate to civilian authority. The Honorable John J. Hamre, former Deputy Secretary of Defense, made it clear that "DoD's mandate is to provide assistance to appropriate federal civilian authority—either the Department of Justice or the Federal Emergency Management Agency." Hamre further stated, "there are no plans to create a 'Homelands Defense Command' or any other military institution to oversee civilian-led response efforts."[78] He was wrong, as the events on September 11, 2001 have changed that special relationship under the newly created Homeland Security Office to which the DoD will be providing assistance through a new command, Northern Command.

Besides, the military's allegiance to the President as Commander-in-Chief makes it the "force du jour" to deliver results without political squabbling. Nonetheless, traditions, ethics and the military ethos compel the military to be sensitive in taking the lead for not impeding citizens' civil rights. As example, Mr. Weiner's August 16, 1999 article in New York Times illustrated this fear stating, "Congress has blocked money for a planned system to safeguard government computers, a prominent Republican has denounced the system as "Orwellian," and some civil libertarians are calling this system a potential threat."[79] One way of avoiding such criticism, while at the same time engaging the nation, is to show the public that the military will take appropriate action to punish those nation states or known terrorists responsible for attacking U.S. homeland's vital interest based on intelligence and military resolve without undue intrusion and curtailment of citizens' civil rights.

At what point then does an attack inflicting damages to U.S. vital interests, but uses non-traditional mechanisms, becomes a proper role for the military? How does this scenario differ from a missile or terrorist attack to one's homeland? One answer is that the U.S. is now working on a national missile defense technology to shoot missiles down in mid-air before it lands on key populated areas. But, the U.S. is not developing a similar defense technology to thwart an information warfare attack, which makes it more difficult to identify the adversary or perpetrator.

The recent designation of U.S. Atlantic Command to U.S. Joint Forces Command continues the tradition of providing military assistance to civil authorities in the event of a nuclear or biological attack within the U.S.[80] An information warfare attack could also fall under this military assistance program. Furthermore, The Armed Forces Journal, October 1999 issue, captured a Marine Corps officer's attitude participating in Exercise URBAN WARRIOR when he said, "I would put down my arms and walk away if the armed forces were to do anything against the American people."[81] This unique feature of respecting the civil rights of the U.S. citizen is a powerful reminder to the military for not assuming lead roles in matters clearly under the auspices of other federal agencies. USA Today recently reported, "the military continues to enjoy the respect from the American public because it does not threaten the interest of any American and it has remained above politics."[82] The message is clear that the military should assume a supporting role in this arena.

Mutual Response

Ultimately, the military support to the community is based on providing basic needs, ensuring public health, providing open communications, and assisting in the rapid return of civil society with its duly constituted government.[83] This is one area the military can touch the hearts and minds of its citizens, and, in turn, win their trust and confidence. The military's ability to

organize and comprehensively respond to crises is a national asset. Therefore, military assistance to public and private sectors is crucial in protecting the well being of the nation. Other lead agencies would be well served to emulate the military's command-and-control structures to achieve unity of effort. Several recommendations are offered here for further exploration:

(1) **Consolidate interagency guidance.** According to the GAO, "Federal Agencies have not completed interagency guidance and resolved command-and-control issues."[84] The Federal Response Plan is a good starting point, but should include annex(es) that deal with information warfare.

(2) **Elevate the title of National Coordinator to Director for Security, Infrastructure Protection and Counter Terrorism.** Put teeth into implementation of Presidential Decision Directive 63 on Critical Infrastructure Protection that covers information warfare attack.[85]

(3) **Keep the private sector engaged.** A dialogue has been initiated via the Information and Sharing Analysis Center (ISAC) that keeps industry engaged. Under the Presidential Decision Directive 63, ISAC was allowed to "gather, analyze, sanitize and disseminate private information from the National Information Protection Center for further distribution to the private sector."[86] The idea was designed so "the ISAC may emulate particular aspects of such institutions such as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors."[87] Despite an exchange of ideas, the private sector is motivated by profit. There must be a "carrot" to get the private sector engaged, otherwise, their full cooperation in strengthening a responsive public-private partnership remains hallow. J. Douglas Beason, author of "DoD Science and Technology," was correct when he said: "Industry will not step up to fill a void unless there is a sufficient profit."[88] Possible incentives for the private sector might be tax breaks or other governmental relief.

(4) **Integrate cyber attack impact to U.S. Joint Forces Command's Joint Task Force for Civil Support.** This training program needs to address strengths and weaknesses of state and local computer defense mechanisms and may require extra efforts since the task force appears to be more focused on dealing with disasters caused by the weapons of mass destruction.

(5) **Integrate the lead agency (Sector Liaison Official) with the private sector (Sector Coordinator).** The coordinator will need to assess and develop a workable course of action.[89] State and local government agencies should maximize benefits offered by the public and private sector at the national level. Ultimately, the objective is to make the public and private sectors more aware of the military support role in their community.

Again, the military role should be supporting, not supported for information warfare defense. An exception to this rule applies if the attack is initiated by rogue nations or known terrorists against U.S. vital interests or conditions where the military is best suited for the mission. For domestic consequence of a such attacks, the military role should also be supporting. The military can perpetually maintain the highest respect and admiration from the U.S. citizen by defending the homeland against such attacks from rogue nation states and known terrorists. Taking the supporting position on the defense of information warfare attack and domestic consequence platform allows the military to distance itself from getting entangled with civil matters affecting domestic law enforcement. At the same time, the military should simultaneously assist agencies to better prepare them against an information warfare attack and improve their homeland information warfare attack defense—a win-win situation for the nation.

Approach to Information War

Attacking adversaries' information systems has always been part of war, and new technological approaches offer more possibilities for doing that both now and in the future. However, the new kinds of weapons that can attack information systems (e.g., computer viruses, microwave weapons) need to be subjected to the same kind of analytic scrutiny as other weapon systems to see where they fit in the overall scheme of things and under what conditions they offer particular advantages. The broader issue is to determine against what kind of adversaries the whole information-intensive approach to war is likely to work well and how likely the U.S. is to have to fight such adversaries. Dealing with this set of analytical issues should enlighten both investment decisions and fundamental questions about how to structure the U.S. national security apparatus. Most offensive information warfare capabilities are close hold, not unlike nuclear weapons. Perhaps a single integrated operational plan (an IW-SIOP) should be developed

against information warfare adversaries. Such a program would benefit by adopting all the attendant surety programs such as the personnel reliability program that requires two-persons at all times when accessing or operating weapon systems.

Managing the organizational side of the transition is important as well. The military should proceed carefully in embracing information technology and in organizing to conduct information operations. Although there are areas the military needs to play serious catch-up, there is a danger in moving too quickly in others and reorganizing prematurely. In particular, new information warfare organizations may miss their niches entirely because of ineffective integration and isolation. On the other hand, established organizations that "talk the talk" might be able to prevent effective organizational advancement if they do not develop a thorough understanding to accompany the jargon. That is why designing information warfare related organizational structures that can adapt is so important and why premature restructuring of organizations is so risky. The military should create organizational structures and processes that will permit an integrated analysis of information-related issues. These structures should permit an evolution toward a more information-dominated world if and when it is warranted. So far the U.S. has avoided some of the worst potential pitfalls, but the battle is just starting. Given the new roles and missions that will be developed for homeland defense, it is more likely that the military will become involved in defense operations reminiscent of the Aerospace Defense Command. This will integrate Guard and Reserves and give them the responsibility for these new mission areas. At the national level, a national level agency, similar to the Defense Intelligence Agency, should be formed to handle information warfare for the nation—both civilian and military.

Information warfare is clearly the current fad that might or might not prove to be the wave of the future. It depends on how events unfold and what rigorous, systematic analysis shows about the relative importance of various elements of information warfare. The real danger is that the "in vogue" aspects could hold back the very trends that could make it the wave of the future. As one particularly astute observer put it:

> The history of information technology can be characterized as the overestimation of what can be accomplished immediately and the underestimation of long-term consequences.[90]

Organization is currently in a burgeoning state of development undergoing changes—a veritable state of flux. With new emphasis on homeland security, one can expect there may be more changes. It is suggested that policymakers give serious considerations to an interagency approach to organization. Some would suggest an Information Warfare Czar at the cabinet level, others a specified Assistant Secretary of Defense. The appropriate approach is to place both military and civilian information warfare under a combined structure not unlike the Defense Intelligence Agency. This allows leaders to discuss, plan, organize and execute information warfare as it impacts both military and civilian worlds. Inattention to one and not the other is inadequate and likely to be unproductive. However, a coherent national policy is first necessary, which the next chapter will discuss.

Notes

[73] Joffe, Josef, *Democracy and Deterrence: What Have They Done to Each Other?* in Miller, Linda B. and Michael Joseph Smith, *Ideas & Ideals: Essays on Politics in Honor of Stanley Hoffman,* Westview Press, Boulder, CO, 1993, pg. 114.

[74] For example, the creation of the Information Warfare Squadron at 9th Air Force illustrated the organizational problems and the complications that jargon can cause. On one hand, creating such a group at an operational command focused attention at the operations level, where it belongs. On the other hand, what was the squadron to do? A squadron cannot handle the scope of information warfare, which the AFDD 2-5 defines as including information operations, defense of information systems, and attack of adversary information systems. Information operations alone include a large part of what the operational Air Force does. A squadron could focus on protecting information systems, but there was already a large directorate (SC) at 9th Air Force that had the manpower and expertise and should logically have had that charter. Some squadrons have found a niche in offensive information operations, an area that is in large part now under AF Space Command. However, offensive information warfare cells should be integrated with the offensive planners who employ more traditional weapons to attack a full

Notes

spectrum of adversary targets, including those associated with information operations. AF Information Squadrons have proven a useful conduit for focusing attention on the needs of the operators for information-related support and providing a suitable organizational focus.

[75] Brewin, Bob, *Kosovo Ushered in Cyber War*, Federal Computer Week, September 27, 1999, pg.1.

[76] Munro, Neil, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, Washington Post, July 16, 1995, pg. C3.

[77] Federal Emergency Management Agency, *Report on Outstanding Issues in Oklahoma City, Oklahoma as Related to the Bombing of the A.P. Murrah Federal Building,* Washington, DC, July 3, 1996.

[78] Hamre, John J., *U.S. Military wants no Domestic Law-Enforcement Role*, USA Today, October 5, 1999, pg. 16.

[79] Weiner, Tim, *Author of Computer Surveillance Plan Tries to Ease Fears*, New York Times, August 16, 1999, pg. 1.

[80] Dorsey, Jack, *Cohen Warns of Perilous Global Times*, The Virginia Pilot, October 8, 1999, pg. B4.

[81] Sherman, Jason, *Invading Virginia*, Armed Forces Journal, October 1999, pg.16.

[82] *Terrorist Attack in U.S? Don't Put Military In Charge*, USA Today, September 30, 1999, pg.19.

[83] Sullivan, Gordon R. and Michael V. Harper, *Seeing the Elephant, Hope Is Not A Method,* Times Books, Chap 5, pg. 85.

[84] *GAO Cites Computer Security Risks*, Washington Post, October 4, 1999, pg.7.

[85] *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 1998, Section IV, *A Public-Private Partnership to Reduced Vulnerability*, August 31, 1999.

[86] *Clinton Administration's Policy*, Appendix F-12.

[87] Sullivan.

[88] Beason, Douglas, *There Ain't No Such Thing As A Free Lunch*, DoD Science and Technology, pg. 98.

[89] *Clinton Administration's Policy*.

[90] Strassman, Paul, *Information Payoff: The Transformation of Work in the Electronic Age*, Free Press, New York, NY, 1985, pg. 199.

Chapter 6

The National Plan—Towards A U.S. CONOPS?

Given the reality of the threat, the vision and policy, the U.S. needs to implement measures that best organize and prepare for offensive and defensive information warfare. With the myriad of Presidential Commissions and numerous White Papers, former President Clinton laid out a framework for the nation—a National Plan for Information Systems Protection. It is no surprise that there is a reluctance to set policy and strategy for the offensive use of information warfare. Its use is seen as a weapon of mass disruption. Analogous to the use of nuclear weapons, policymakers are taking a cautionary approach to strategies as they did during the Cold War. In any case, U.S. policy is one that must reserve the "right to strike" whenever the U.S. may find itself under information warfare attack.

It is said that "the best offense is a good defense" and vice versa. This monograph has pointed out that the U.S. is the single largest information user with untold vulnerabilities inside its information infrastructure. To that end, the National Plan was developed to take steps to protect vital "information" interests and defend against such attacks against the U.S. information infrastructure. The President ordered that the Federal Government to become the model of computer system security, which to date it is not. The DoD is well on its way to creating secure systems, but civilian Agencies are also critical and are generally poorly protected from computer system attack. The National Plan proposed additional steps to be taken by DoD and by the rest of the Federal Government.

The private sector information infrastructure is at least as likely to be the target for computer system attack. Throughout the modern era, and past wars, critical industries and

utilities have always been targets for destruction in conflicts. U.S. strength rests on its privately owned and operated critical infrastructures and industries. Even now, privately owned computer networks are being surveyed, penetrated, and in some cases made the subject of vandalism, theft, espionage, and disruption. While the President and Congress can order Federal networks to be secured, they cannot and should not dictate solutions for private sector systems.

The National Plan[91]

The National Plan does not lay out in great detail what will be done to secure and defend private sector networks, but suggests a common framework for action. Already some private sector groups have united to defend their computer networks. The government can and should help them, but should not dictate solutions and avoid undue regulation. Nor should it infringe on civil liberties, privacy rights, or proprietary information. But it must mandate that these systems be protected. Infrastructure assurance goals can be accomplished in a manner that is consistent with the full range of civil liberty interests. Some infrastructure assurance programs should have a positive impact on personal privacy, and civil liberties, by enhancing the level of security in data and communications in networked environments. The bottom line is the government has a solemn obligation to protect the private information of its citizens that resides on its computers. Private industry should have a similar responsibility.

The National Plan takes into account the risk that technologies designed to protect information and systems, if not carefully utilized, could accidentally undermine civil liberties. Even with the best of intentions technology that protects against intrusions, when cast too broadly, could profile innocent activity. Where individual rights are at issue, careful consideration of all related issues is essential because the legal precedent does not always offer clear guidance in areas of jurisdiction, security standards, and consent issues. Information

attacks often raise complicated legal and jurisdictional issues; consequently, government programs that protect infrastructures and civil liberties require careful planning, analysis, and input from all affected participants.

While all the proposals in the National Plan were developed in a manner consistent with existing law and constitutionally guaranteed expectations of privacy, portions may give rise to concerns that personal privacy rights may be sacrificed in exchange for infrastructure assurance objectives. Finding solutions to infrastructure assurance in a manner consistent with civil liberties is a vital process that must involve both government and private sector communities. This process recognizes the complexity and importance of existing jurisprudence and work to structure new programs to prevent unintended consequences.

Goals

The goal of the National Plan is to achieve a critical information systems defense. To meet the ultimate goal established by PDD-63 for defending the Nation's critical infrastructures against deliberate attack by 2003, the National Plan is designed around three broad objectives:

- ***Prepare and Prevent***: Those steps necessary to minimize the possibility of a significant and successful attack on critical information networks, and build an infrastructure that remains effective in the face of such attacks.
- ***Detect and Respond***: Those actions required identifying and assessing an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.
- ***Build Strong Foundations***: Those actions one must do as a Nation to create and nourish the people, organizations, laws, and traditions which will make us better able to Prepare and Prevent, Detect and Respond to attacks on critical information networks.

The National Plan proposes ten programs for achieving these objectives that include:

Prepare and Prevent

- Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities

Detect and Respond

- Program 2: Detect Attacks and Unauthorized Intrusions.
- Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.
- Program 4: Share Attack Warnings and Information in a Timely Manner.
- Program 5: Create Capabilities for Response, Reconstitution, and Recovery.
- Program 6: Enhance Research and Development in Support of Programs 1-5.
- Program 7: Train and Employ Adequate Numbers of Information Security Specialists.
- Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber-Security.
- Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8.
- Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.[92]

The Programs

The ten programs aimed at achieving the National Plan goals and objectives are captured below:

Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities.

The Government and the private sector will identify significant assets, interdependencies, and vulnerabilities of critical information networks to attack, then develop and implement realistic programs to remedy the vulnerabilities, while continuously updating the assessment and remediation effort. The initial necessary step in preparing a defense of critical information systems and computer networks is a thorough assessment of potential critical infrastructure system assets, interdependencies, and vulnerabilities.

Recommended practices and standards for information systems security can assist organizations in their efforts to identify and address vulnerabilities. While much has been done, a common framework of information systems security recommended practices and standards is still in its infancy. Close cooperation between the Federal Government, the private sector, and standards-setting bodies will lead to a more robust and accepted set of guidelines for

organizations to follow in identifying vulnerabilities and prioritizing remedial actions. Recognizing that all vulnerabilities cannot be remedied immediately due to both technical and fiscal constraints, Government and private sector groups must prioritize remediation efforts, based on the critical assets and interdependencies analysis throughout the next five years.

Program 2: Detect Attacks and Unauthorized Intrusions.

This program installs multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers (first in DoD, then the Federal Intrusion Detection Network (FIDNet) in coordination with other Federal Agencies) will receive warnings from these detection devices. In addition to Computer Emergency Response Teams (CERTs) and other means, these warnings will be used to analyze and defeat attacks.

Given the vulnerability of systems and software, the number of target systems, and the frequency of unauthorized intrusions, the development and deployment of detection and monitoring systems are crucial. These intrusion detection systems are already in use in the Executive Branch and Congress. Networking intrusion detection monitors across Federal Departments and Agencies with a central capability to analyze system anomalies is a key next step in enhancing system security. Installing intrusion detection monitors and defensive detection systems are among the first steps necessary to detect unauthorized intrusions or activities on a network.

The National Plan calls for the installation of the "best of breed" program in each of the four types of defensive detection systems where appropriate on critical information system

networks. Such installation is mandated within the Government, which will also share evaluations of such systems through Information Sharing and Analysis Centers (ISACs).

Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.

This program assists, transforms, and strengthens U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal, one that acts against computer networks.

In the past, the overseas threat to the U.S. infrastructure at home was from bombers, intercontinental missiles, and submarines. Those systems could be located and counted by intelligence agencies. Now, the threat to the U.S. infrastructure from computer-based attacks can originate from capabilities and locations that are much more difficult to find and assess. U.S. Intelligence Agencies are given high priority for collection of information on foreign information warfare capabilities and intentions, consistent with Executive Order 12333, Attorney General Guidelines, and Director of Central Intelligence directive protocols.

Information warfare attack threats pose a different and more difficult challenge than intelligence collection about traditional military threats. Proving that an attack has taken place, finding out who has done it, and proving guilt requires new skills and the sound integration of law enforcement, intelligence analysis, and national security responses. The National Infrastructure Protection Center (NIPC) at the FBI is an interagency center using information from all sources, including open sources, the private sector, law enforcement, and the U.S. Intelligence Community, to provide early warning of attacks and to respond in part by gathering information necessary to identify the responsible party. NIPC has both law enforcement and Foreign Counter-intelligence missions, and operates under authorities that cover activities in both

of these areas. NIPC has representatives from DoD, Intelligence, NSA, and other Federal Agencies and is taking the lead to develop and improve capabilities to determine when an attack has taken place, analyze the scope and origins of an attack, and find the perpetrator(s).

Warnings of possible attacks, and appropriate incident and vulnerability data, will be shared with the private sector and state and local governments. This information is critical to efforts that improve their defenses against attack. The Government will also work closely with trusted law enforcement counterparts from other nations to build a system of enhanced international cooperation, and develop a common approach to criminalizing unauthorized intrusions and attacks on critical information systems. Policies and programs will be developed consistent with existing rules and policies concerning the permissible roles of domestic law enforcement and national security agencies for domestic and foreign activities, respectively.

Program 4: Share Attack Warnings and Information in a Timely Manner.

When the "Solar Sunrise" attack on Air Force computers was first noted in February 1998, there were inadequate procedures or methods of knowing whether such attacks were ongoing against other DoD systems, key networks, or critical private sector systems. The National Plan calls for a more effective nationwide system to pass information in real time about attacks.

Program 5: Create Capabilities for Response, Reconstitution, and Recovery.

This program is designed to limit an attack while it is underway and to build into corporate and agency continuity and recovery plans the ability to deal with information attacks. Information warfare attacks may not be limited in their scope to isolated incidents. They may be directed at an entire industry or agency, a whole sector of the economy, a region of the country, or the Nation itself. Once a widespread attack has been identified, the Centers may work in

concert with law enforcement and other agencies to initiate a response. Their response will include recommendations to systems managers to implement pre-planned measures that:

- Block access to their networks by suspect users.
- Initiate "defense condition" security precautions not normally employed.
- Apply new security software "patches" aimed at the attack technique.
- Isolate elements of the network.
- Suspend operations of portions of the network.
- Commence operations of emergency continuity systems.

Simultaneously, law enforcement and other agencies will locate the origin of the attacks and take appropriate measures to terminate them. The private sector and law enforcement will consult on response so that the private sector reaction does not needlessly hamper or eliminate the possibility of investigation of the intrusion, attribution to the accountable parties, and if possible, prosecution of the offender(s).

The goal for Government and the recommendation for industry is that every critical information system have a response plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems. Plans usually include "back-up" computer databases in case the headquarters system is unavailable. However, recovery plans must be designed for contingencies when all or part of the information network is itself compromised. Alternative methods of passing minimal essential information must be available. Expert teams must be quickly available to assist in reconstitution efforts, including analyzing software problems disabling the network, designing alternative avenues, and reinitiating network operations.

Program 6: Enhance Research and Development in Support of Programs 1-5.

This program systematically establishes research requirements and priorities needed to implement the National Plan, ensures funding, and creates a system to make certain that information security technology stays abreast with changes in the threat and in overall information systems.

Many of the tasks required in the first five steps of the National Plan cannot be performed well or not all with today's technology. The interagency Critical Infrastructure Coordination Group has created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy, the Research and Development Sub-Group works will work with Agencies and the private sector to:

- Gain agreement on requirements and priorities for information security research and development.
- Coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts.
- Communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia.
- Identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

Program 7: Train and Employ Adequate Numbers of Information Security Specialists.

This program will survey the numbers of people and the skills required for information security specialists within the Federal Government and nationwide, and take action to train current Federal information technology (IT) workers and recruit and educate additional personnel to meet shortfalls.

Nationwide, evidence suggested a growing danger of a shortage of skilled IT personnel. Within the subset of information systems security personnel, the shortage is acute. Within the Federal Government, the lack of skilled information systems security personnel amounts to a

crisis. This shortfall of workers reflects a shortage of university graduate and undergraduate information security programs. In addressing these problems, the U.S. must leverage the ongoing efforts made by the DoD, NSA, CIO Council, and various Federal Agencies.

Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber-Security.

This program will publicly explain the need to act before a catastrophic event and to improve the ability to defend against deliberate information attacks. Defending U.S. cyberspace requires action by all U.S. citizens, business leaders, education and other private sector institutions, the government (Federal, state, and local), and ultimately, the general public. The foundation for the many actions, outlined in the National Plan, is the understanding and awareness of the new threats posed to U.S. information systems, and the need for action.

There has been, so far, no "electronic Pearl Harbor" to galvanize public awareness about the need for action. Nor do many U.S. citizens appreciate the extent to which the economy and national security now depend on computers and information systems. Often times this functionality is hidden from everyday life. Consequently, a broad reaching public awareness effort is needed. In the initial phase, this will include at least three elements:

- Educating the youth about cyber-ethics and appropriate behavior and use of the Internet and other communications tools through the *CyberCitizens Progra*m.
- Forging a partnership with corporate and information technology leaders, the *Partnership for Critical Infrastructure Securit*y, in which one jointly acknowledges the need to take specific action to improve U.S. cyber-security in the private sector and the government.
- Ensuring that Federal employees are themselves a model of awareness of the need for information systems security.
- Building on the above elements, extending the awareness campaign to reach other private organizations and the general public.

These actions are the foundation for ensuring the national commitment to proactively defend U.S. information-based infrastructures.

Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8.

This program develops the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation between the Federal Government, including Congress, and private industry. There are proposed initiatives that direct Federal Departments and Agencies to make their own critical systems secure and build a partnership with the private sector to protect U.S. infrastructures. Congressional members and committees have demonstrated that they share the perception of the potential dangers from attack on U.S. critical cyber-driven systems, and give high priority to taking protective actions. Existing laws are under review along with previously introduced legislation and developed packages of new proposals designed to promote security of critical infrastructures.

The government must be able to protect sensitive information and alleviate potential liability and antitrust concerns associated with sharing such information by and with private industry. As identified in the other programs, new legislation is needed to build the foundation partnership between industry and Government and facilitate the formation of private sector ISACs and information sharing in the private sector with the government.

Further, the U.S. must develop appropriate legislative frameworks that promote interim and full operating capability to protect critical systems. Congressional support for future President's budgets to fund the National Plan is paramount because success in meeting the milestones established in the National Plan is dependent upon the level of funding.

Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.

This key program is incorporated in all the programs and is making protection of critical cyber systems conform to Constitutional and other legal rights. While safeguarding U.S. critical infrastructures is vital, protecting civil liberties is paramount. All the proposals in the National Plan have been developed in a manner fully consistent with existing law and expectations of privacy. The National Plan calls for annual public-private colloquiums on Cyber Security, Civil Liberties, and Citizen Rights to ensure that those implementing the National Plan remain sensitive to civil liberties and that they share their proposals on cyber security with those inside and outside of Government with expertise and concern for citizen rights.

The National Infrastructure Assurance Council, a board of individuals from outside of the Federal Government, will be tasked to conduct an annual review of implementation of the National Plan relative to civil liberties, privacy rights, and proprietary data protection. The design of the National Plan incorporates privacy protections established by Fourth Amendment jurisprudence. Any action by the Government to search a citizen's computer or the content of electronic communications must be in accordance with existing laws, such as the Electronics Communications Privacy Act.

The U.S. continues to wrestle with establishing clear conceptual and doctrinal frameworks for fitting information warfare into its national security policy. The establishment of organizations to deal with transformational information warfare roles and missions has proven difficult. U.S. efforts to mange these organizational challenges has been slow. There is a lack of open information available regarding specific organizational arrangements for U.S. strategic information warfare efforts; however, the National Plan is a step forward towards developing organizational arrangements and a unified national concept of operations.

Conclusion

It is clear that information can be used as a weapon, but strategists must use it with judiciously. It is not the prophetic "silver bullet" weapon. It could be used alone or be used in concert with more traditional weapons. It could be employed as a precursor weapon that could blind an adversary prior to conventional attacks and/or operations. There is a need for educating strategists of possible offensive information warfare actions that can be identified and analyzed prior to integration with more traditional weapons. Although offensive actions should be closely integrated with defensive measures, offensive capabilities (as well as the adversary's) should be the driver for defensive actions. One should have both offensive and defensive capabilities.

There is no firm set of criterion to evaluate an information warfare attack to determine if it is an act of war. Such a list of criteria would be nice, but is not possible due to the inherent ambiguity in such attacks and the attendant requirement to rely on perception to judge an act as warlike. However, with sufficient information, a response in kind can be launched. Worldwide publicity can be invoked against the attacker with the U.S. explanation dominant. Such an explanation should include the phrase "act of war" to generate the impression in the targeted audiences the perceived severity without actually declaring war. This is the same action taken recently in the U.S. response to the World Trade Center terrorist attacks. Such actions follow the principle of military necessity as well as proportionality outlined in the Law of Armed Conflict.

An information warfare weapon as mass disruption may never equate to a weapon of mass destruction until such major information warfare attacks have been launched and the public can see, feel, and evaluate the results. Perception is the name of the game, especially with a worldwide audience watching. The definition of war in this new information age of global

networks, transnational commerce, and increasing blurring of borders is changing and being debated. At the very core of any nation-state's view of war should be a National Information Policy that clearly defines intangible values, ethical positions, and national security thresholds that would trigger a countervailing response. Such policy must include options for dealing with renegades, terrorists, corporations or individuals who provoke the international community outside the control of their nation-state hosts.

Preparing for strategic information warfare requires developing concepts about the conduct of such warfare. While many hypothetical scenarios and exercises have been devised, no publicly acknowledged conflict between actors based upon strategic information warfare has yet occurred. As with other uses of force, adversaries can usefully conceive of the strengths, weaknesses, and vulnerabilities of this new form of warfare for achieving offensive, defensive, and deterrent objectives. Strategically, information warfare appears to involve the same enabling conditions for success necessary for waging strategic nuclear warfare in the past. Yet mass disruption caused by an information warfare attack may prove difficult to estimate. The widespread availability of the means for disrupting information infrastructures has led to a belief that almost anyone can obtain and employ the tools for waging information warfare. Yet, establishing effective defensive, and especially offensive, military capabilities has not proved to be so straightforward. The technologies for information warfare and control of infospace differ from the past. Instead of a military monopoly on nuclear weapons, there are rapid developments of commercial technologies that shape the operational environment for information operations. While technological tools, in the form of information warfare weapons, have become easily accessible, developing organizations that can effectively wield such weapons to conduct offensive and defensive missions poses major obstacles.

Some Final Recommendations

Successful strategic information warfare attacks rely on the ability of offensive forces to achieve access to targeted centers of gravity. U.S. dependence on widely commercial available products is a huge vulnerability to mass disruption. The characteristics of these vulnerabilities and information warfare weapons are quickly distributed among potential attackers. Those responsible for protecting information infrastructures across U.S. society should implement the following recommendations:

1) The U.S. should establish a declaratory deterrence policy related to strategic information warfare that clearly states the U.S. willingness to respond with the range of military forces at its disposal in response to information warfare attacks against both state and non-state actors who threaten the national physical and economic security.
2) Establish a U.S. national policy to improve strategic information warfare defense that stresses the voluntary, fast disclosure of vulnerabilities once discovered by the broad range of technology producers, network administrators, and infrastructure users.
3) Share lessons learned from the active efforts ongoing within the U.S. national security community to protect its information infrastructures and feed them into the policy framework.
4) The national security community should clearly and publicly communicate the threat posed by strategic information warfare at the highest levels, including the NCA, to stimulate responses across all sectors of society beyond the everyday common computer security risks
5) The U.S. government must strengthen institutions that collect information on infrastructure vulnerabilities and develop remedial measures. Such reported information will remain confidential to minimize concerns over reputation, legal liability, privacy, national security, and potential; punitive actions.
6) Improve efforts by operators and users to implement fixes that reduce the systemic sources of vulnerability to strategic information warfare attacks within the U.S.. Policies should be developed that create legal requirements for due diligence by operators and users activity related to the security and reliability of information infrastructures.
7) The U.S. government should create educational programs that improve the skills of security specialists and system administrators responsible for assessing and repairing problems throughout the U.S. information infrastructure.
8) The U.S. should manage the risk posed by strategic information warfare attacks through deterrence by establishing linkages to its varied sources of strength and developing strong defensive measures to protect it against such attacks. This includes developing the ability to retaliate in-kind through offensive information

warfare measures. These measures must provide the most credible threat against potential adversaries with significant information infrastructure-based vulnerabilities.

9) The U.S. should establish international legal norms regarding the conduct of information warfare that improves the legitimacy and credibility of retaliatory threats. Such regimes must address the potential for non-state actors to possess and use information warfare capabilities.
10) The U.S. must improve its understanding of its potential adversaries, state or non-state actors, in the realm of strategic information warfare. Effective U.S. strategic information warfare defenses must also account for differences among these potential adversaries.
11) U.S. policy should encourage cooperative, proactive measures by the private sector to limit vulnerabilities in the technological baseline of information infrastructures to enhance the overall strength of its strategic information warfare defenses.

These measures can establish the baseline for both offensive and defensive strategic information warfare actions that will protect U.S. information infrastructures while offering a strong deterrence to possible adversaries. At the very least, more research, analysis, modeling, and debate are warranted. Vision, policy, and strategy are vital to the overall success of any venture, private or military, and in the case of strategic information warfare these are essential tools to an effective offense and defense. Strategic information warfare can be a weapon of mass disruption and in treating it as such; there are similarities to U.S. nuclear policies and strategies that can be helpful to understanding bytes—weapons of mass disruption.

Annex A. Example IW Weapons[93]

Computer Viruses

A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces. As computers switch today's telephone systems, you can shut them down, or at least causing massive failure, with a virus as easy that you can shut down a "normal" computer.

Worms

"A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs." Also if worms don't destroy data they can cause the loss of communication with only eating up resources and spreading through the networks. A worm can also easily be modified so that data deletion or worse occurs.

Trojan horses

A Trojan horse is a code fragment that hides inside a program and performs a disguised function. It's a popular mechanism for disguising a virus or a worm. A Trojan horse could be camouflaged as a security related tool for example like SATAN (Security Administrating Tool for Analyzing Networks). SATAN checks UNIX systems for security holes and is freely available on the Internet. If someone edits this program so that it sends discovered security holes in an e-mail message back to him the person learns much information about vulnerable hosts and servers. A

clever written Trojan horse does not leave traces of its presence and because it does not cause detectable damage, it is hard to detect.

Logic bombs

A bomb is a type of Trojan horse, used to release a virus, a worm or some other system attack. It's either an independent program or a piece of code that's been planted by a system developer or programmer. Its activation could also be triggered from the outside. An effect could be to format the computers hard disks.

Trap doors

A trap door, or a back door, is a mechanism that's built into a system by its designer. The function of a trap door is to give the designer a way to sneak back into the system, circumventing normal system protection. A trap door could allow the designer to explore systems and the stored data of any type.

Chipping

Just as software can contain unexpected functions, it is also possible to implement similar functions in hardware. Today's chips contain millions of integrated circuits that can easily be configured by the manufacturer so that they also contain some unexpected functions. They could be built so that they fail after a certain time, blow up after they receive a signal on a specific frequency, or send radio signals that allow identification of their exact location. The main problem with chipping is that the specific (adapted) chip be installed in the place that is useful

for the information warrior. The easiest solution is to built the additional features into all the chips manufactured in the country that is interested in this type of IW.

Nano machines and Microbes

Nano machines and Microbes provide the possibility to cause serious harm to a system. Unlike viruses, one can use these to attack not the software but the hardware of a computer system. Nano machines are tiny robots that could be spread at an information center of an adversary. They crawl through the halls and offices until they find a computer and are so small that they enter the computer through slots and shut down electronic circuits. Another way to damage the hardware is a special breed of microbes. They could destroy all integrated circuits in a computer lab, a site, a building, and a town.

Electronic jamming

Electronic jamming is used to block communications channels at the adversary's equipment so that they can't receive any information. The next step is not to block their data traffic, but instead overwhelm them with incorrect information. This type of disinformation can also be combined with other types of IW attacks."

HERF Guns - EMP Bombs

HERF, High Energy Radio Frequency, guns are able to shoot a high power radio signal at an electronic target and put it out of function. The damage can be moderate (e.g. that a system shuts down, but can be restarted) or severe (e.g. the system hardware has been physically damaged). Electronic circuits are more vulnerable to overload that most people would suspect. This

mechanism uses HERF guns with big success. I n essence, HERF guns are nothing but radio transmitters that send a concentrated radio signal to the target. The target can be a mainframe inside a business building, an entire network in a building, or as today's planes and cars are stuffed with electronic equipment, the target can even be a moving vehicle with all the inherent dangers for the people who are inside.

EMP stands for electromagnetic pulse. The source can be a nuclear or a non-nuclear detonation. Special forces teams who infiltrate adversary territory and detonate a device near their electronic devices can use it. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF gun to cause a similar amount of damage and is typically used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb.

Notes

[91] *Defending America's Cyberspace, The National Plan for Information Systems Protection, Version 1.0*, The White House, Washington, DC, 2000. What is presented is a synopsis taken directly from the text of the National Plan.
[92] Ibid.
[93] Russel Deborah and Gangemi G.T., *Computer Security Basics*, O'Reilly & Associates, 1994.

Annex B. Common Definitions

Command-and-control Warfare — The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command-and-control capabilities, while protecting friendly command-and-control capabilities against such actions. Command-and-control warfare is an application of information warfare in military operations and is a subset of information warfare. Command-and-control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive:

a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.

b. C2-protect. Maintain effective command-and-control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command-and-control; electronic warfare; intelligence; military deception; operations security; psychological operations. (JP 3-13.1)

Cyber attack-- Any attack through cyber-means to intentionally affect national security (cyber warfare) or to further operations against national security. Includes information warfare attacks by unintentional actors prompted by intentional actors. (Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp. 141-165).

Cyberwar—any act intended to compel an opponent to fulfill U.S. national will, executed against the software controlling processes within an opponent's system. It includes the following modes of information warfare attack: infiltration, manipulation, direct assault, or raid. Infiltration is the penetration of the defenses of a software-controlled system such that the system can be manipulated, assaulted, or raided. Manipulation is the control of a system via its software that leaves the system intact, and then uses the capabilities of the system to do damage. For example, using an electric utility's software to turn off power. An assault is the destruction of software and data in the system, or attack on a system that damages the system capabilities. Includes viruses, overload of systems through e-mail (e-mail overflow), etc. Finally, a raid is the manipulation or acquisition of data within the system that leaves the system intact and results in transfer, destruction, or alteration of data. For example, stealing e-mail, cookies, IP addresses, or taking password lists from a server. Also **cyberwarfare**. (Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp. 141-165).

Cyberspace—the impression of space and community formed by computers, computer networks, and their users; the virtual world that Internet users inhabit when they are online. (Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp. 141-165). It is the notional environment in which digitized information is communicated over computer networks. (JP 2-01.3)

Information warfare — Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called **IW.** (JP 3-13).

Netwar—spans economic, political, social, and military forms of war. In contrast to economic wars that targeted the production and distribution of goods, and political wars that aim at the leadership and government infrastructure, netwar would be distinguished by its deliberate targeting of information and communications. This warfare seeks to disrupt, deceive or deny targeted information. It refers to information related conflict at a strategic level. (Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp. 141-165).

Offensive IO [warfare] involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives. These assigned and supporting capabilities and activities include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack.

Offensive IO [warfare] may be conducted in a variety of situations and circumstances across the range of military operations and may have their greatest impact in peace and the initial stages of a crisis. Beyond the threshold of crisis, offensive IO can be a critical force enabler for the JFC.

Offensive IO may be conducted at all levels of war — strategic, operational, and tactical — throughout the battlespace. (JP 3-13)

Weapons of mass destruction — Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called **WMD.** (JP 1-02)

Weapons of mass disruption — weapons of information warfare characterized as weapons of mass disruption, which may include various forms of malicious code, perception management activities, and flexible deterrent options. Malicious code is broken into four categories: viruses, worms, Trojan horses and logic bombs. These weapons offer remarkable attack potential at a low cost and low risk. Targets may include hardware, software, firmware, wetware, information, or any combination. Other high technology disruptive weaponry, such as mass spectrum directed energy weapons and surgically precise low power particle beam weapons that cause disruption through destruction of key components in an adversary's information systems.

Bibliography

Advance Planning Briefing for Industry, Winning the Information War, United States Army Communications- Electronics Command, Fort Monmouth, New Jersey. Symposium held May 11-12, 1994, Ocean Place Hilton Resort and Spa, Agenda and Description of Sessions, 10 pages.

Alberts, David S., *Defensive Information Warfare*, National Defense University, NDU Press, Washington, DC, August 1996.

Alberts, David S. and Garstka, John J., *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition, CCRP Publication series, Washington, DC, August 1999.

Alberts, David S. and Papp, Daniel S., *Volume II of Information Age Anthology: National Security Implications of the Information Age*, CCRP publication series, Washington, DC, August 2000.

Alberts, David S. and Papp, Daniel S., *Volume III of Information Age Anthology: The Information Age Military*, CCRP publication series, Washington, DC, March 2001.

Anderson, Kent, *Intelligence Based Threat Assessments for Information Networks and Infrastructure: A White Paper*, Global Technology Research, Inc., Portland, OR, 1998.

Arquilla, John and Ronfeldt, David, *Cyberwar is Coming!*, The Journal Comparative Strategy Taylor & Francis, Bristol, PA, Volume 12, no. 2, 1993, pp. 141-165.

ASPC Paper Number 47, Military Information Operations in a Conventional Warfare Environment, Air Power Studies Centre, Commonwealth of Australia, 1995.

Benedickt, Michael Ed, *Cyberspace - First steps*, MIT Press. Cambridge, MA, 1991.

Bennett, Sheila G., Captain, USAF, *A Process for Vectoring Offensive Information Warfare as a Primary Weapon Option within the Unites States Air Force*, AFIT/GER/ENS/01M-01, Air Force Institute of Technology, Wright-Patterson AFB, OH, 2001.

Buchan, Glenn, *Information War and the Air Force: Wave of the Future? Current Fad?*, Issue Paper, Rand Publications, Santa Monica, CA, March 1996.

Builder, Carl H., *The Icarus Syndrome: The Role of the Air Force in the Evolution and State of the U.S. Air Force*, Transaction Publications, New Brunswick, NJ, 1994.

Burdea, Grigore and Coiffet, Phillipe, *Virtual Reality Technology*, John Whiley and Sons Inc. New York, NY, 1994.

Cajigas, Anthony, *The Secret Battle Field: Computer Warfare Contingencies II*, Infowar.Com & Interpart Inc., Seminole, FL, September 1997.

Campen, Alan D., ed., *The First Information War*, AFCEA International Press, Fairfax, VA, USA, October 1992.

Clements, Stacy M., Captain, USAF, *The One With The Most Information Wins? The Quest For Information Superiority*, AFIT/GIR/LAL/97D-5, Air Force Institute of Technology, Wright-Patterson AFB, OH, 1997.

Cook, Lt. Col. Wyatt C*., Information Warfare: A New Dimension in the Application of Air and Space Power*, 1994 CJCS Strategy Essay Writing Contest Entry, Air War College, Maxwell AFB, AL, 1994.

Copeland, Thomas E., *The Information Revolution and National Security*, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, August 2000.

Cramer, Myron L., *Information Warfare: a Consequence of the Information Revolution*, class notes from Georgia Tech graduate seminar on the Information Revolution, October 1995

Davis, Norman C., Major, USMC, *An Information Based Revolution in Military Affairs*, Marine Corps University, Quantico, VA, May 1998.

Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue, The White House, Washington, DC, 2000.

DeLanda, Manuel, *War in the age of Intelligent Machines*, Zone Books Swerve edition New York, NY, 1991.

Demchak, Chris, *Military Organizations, Complex Machines- Modernization in the US Armed Services,* Cornell University Press, Cornell, NY, 1991.

Devost, Matthew G., *National Security in the Information Age*, University of Vermont, Burlington, VT, May 1995.

Dretske, Fred, *Knowledge and the Flow of Information*, MIT press Cambridge MA, 1981.

Dunlap, Charles J., Jr., *21st Century Land Warfare: Four Dangerous Myths*, Parameters, U.S. Army War College Quarterly, Autumn 1997, Carlisle Barracks, PA, 1997.

FitzGerald, Mary C., *Russian Views on Information Warfare*, American Intelligence Journal, Spring-Summer 1994.

Forno, Richard F., *The Electronic Battlefield: The Strategic Implications of Information Operations*, Washington Navy Yard, Washington DC, 1996.

Gillam, Mary M., Major, USAF, *Information Warfare: Combating The Threat In The 21st Century*, AU/ACSC/0603/97-03, Air University, Maxwell Air Force Base, AL, March 1997.

Hammonds, Grant T., *The Mind of War: John Boyd and American Security*, Smithsonian Press, Washington, DC, 2001

Horony, Mark D., Captain, USAF, *Information System Incidents: The Development Of A Damage Assessment Model*, AFIT/GIR/LAS/99D-5, Air Force Institute of Technology, Wright-Patterson AFB, OH, 1999.

Hurska, Jan, *Computer Viruses and Anti-Virus Warfare*, Ellis Horwood Publishers. New York, NY, 1990.

Information Applications, New World Vistas: Air and Space Power for the 21st Century, USAF Scientific Advisory Board, New World Vistas Study, United States Air Force, 1995.

Jacobson, Mark R., *War in the Information Age: International Law, Self Defense, and The Problem of "Non-Armed" Attacks*, Mershon Center, Ohio State University, Columbus, OH, 1997.

Johnson, Craig L., *Information Warfare - Not a Paper War*, Special Report, Journal of Electronic Defense, August '94, pp. 55-58.

Johnson, Scott, *Toward a Functional Model of Information Warfare*, Infowar.Com & Interpart, Inc., Seminole, FL, 1992.

Joint Pub 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001.

Joint Pub 3-13, *Joint Doctrine for Information Operations*, October 1998.

Kaplan, Fred, *Reagan's Nuclear Defense Strategy: Myth And Reality*, Policy Analysis No. 6, Washington, DC, January 30, 1982.

Kelly AFB, Tex., *EW Expands Into Information Warfare*, Electronic Warfare, Aviation Week & Space Technology, October 10, 1994, pp. 47-48.

Laurel, Brenda, *Computer as Theater*, Addison-Wesley Publishing. Reading, MA, 1991.

Libicki, Martin C., *Defending Cyberspace and Other Metaphors*, National Defense University, NDU Press, Washington, DC, February 1997.

Lindner, Blake F., Lt Col, USAF, *Information Operations: America's Plan For Strategic Failure*, AU/AWC/161/1998-04, Air University, Maxwell Air Force Base, AL, April 1998.

Luoma, William M., *Netwar: The Other Side of Information Warfare*, Naval War College, Newport, RI, February 1994.

Maj Steven P. Ernst, USAF, Maj Kang Hosug, ROKAF, Maj Frank J. Rossi, Jr., USAF, and Maj Keith A. Thompson, *USAF, Nuclear Strategy And Arms Control: A Comparison*, ACSC/DEA/108/96-04, Air University, Maxwell Air Force Base, AL, April 1996.

Miller, Robert D., Major, USAF, *International Law How It Affects Rules Of Engagement and Responses In Information Warfare*, AU/ACSC/0217/97-03, Air University, Maxwell Air Force Base, AL, March 1997.

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A., *Strategic Information Warfare: A New Face of War*, MR661, Rand Publications. Santa Monica, CA, March 1996.

Munipalli, Seshagiri, Major, USAF, *Information Operations: Moving From Doctrine To Execution*, AU/ACSC/239/1999-04, Air University, Maxwell Air Force Base, AL, April 1999.

Planning Considerations for Defensive Information Warfare: Information Assurance, Defense Information Systems Agency, Arlington, VA, 16 December 1993.

Richards, Dr. Charles W., *Rising the Tiger: What You Really Do With OODA Loops*, Inforwar.Com & Interpart Inc., Seminole, FL, September 1997.

Rosen, Stephen, *Winning the Next War - Innovation and the Modern Military*, Cornell University Press, Cornell, NY, 1991.

Roos, John G., *Info Tech Info Power*, Armed Forces Journal International, Washington, DC, June 1994.

Schechtman, Gregory M., Captain, USAF, *Manipulating The OODA Loop: The Overlooked Role Of Information Resource Management In Information Warfare*, AFIT/GIR/LAL/96D–10, Air Force Institute of Technology, Wright-Patterson AFB, OH, 1996.

Schwartau, Winn, *Information Warfare - Chaos on the Electronic Superhighway*, Thunder's Mouth Press, New York, NY, 1994.

Szfranski, Richard, Colonel, USAF, *A Theory of Information Warfare*, Airpower Journal, Air University, Maxwell AFB, AL, Spring 1994, pp. 56-65.

Thrasher, Roger Dean, *Information Warfare: Implications for Forging the Tools*, Naval Postgraduate School, Monterey, CA, June 1996.

Toffler, Alvin & Heiddi. *War and Anti War,* Little Brown, Boston, MA, 1993.

Van Creveld, Martin. *Command In War*, Harvard University Press, Cambridge, MA, 1985.
Whitehead, Yulin G., *Information As A Weapon: Reality Versus Promises*, School Of Advanced Airpower Studies, Air University, Maxwell Air Force Base, AL, June 1997.

Widnall, Sheila E and Fogleman, Ronald R., General, USAF*, Cornerstones of Information Warfare*, Department of the Air Force, 1996.